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

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	2299 8641 6845 657
Call-Off Contract reference	LEGO 213
Call-Off Contract title	Case Management Managed Service on Azure
Call-Off Contract description	A Managed Service providing ongoing support and continuous improvement to the technical Infrastructure of the Legal Ombudsman.
Start date	01 March 2021
Expiry date	28 February 2023
Call-Off Contract value	£1,645,461.90 ex VAT ()
Charging method	BACS Transfer
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 Secretary of State for Justice (102 Petty France London SW1H 9AJ)** **for the benefit of the Legal Ombudsman (Edward House, Quay Place Edward Street, Birmingham, B1 2RA) ("The CUSTOMER"**)
To the Supplier	Version 1 Solutions Ltd +44 (0)1543 444707 Grosvenor House, Prospect Hill, Redditch, Worcestershire, B97 4DL Company number: 3438874
Together the 'Parties'	

Principal contact details

For the Buyer:

Buyer	The Legal Ombudsman "**Buyer**"
Buyer Address	Edward House, Quay Place, Birmingham, B1 2RA
Invoice Address	Edward House, Quay Place, Birmingham, B1 2RA

Principal Contact	[REDACTED]

For the Supplier:

Supplier	Version 1 Solutions Limited "**Supplier**"
Supplier's Address	Tame House, Wellington Crescent, Lichfield, Staffordshire, WS13 8RZ
Account Manager	[REDACTED]

Call-Off Contract term

Start date	This Call-Off Contract Starts on 01 March 2021 and is valid for 24 months
Ending (termination)	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). 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).

Extension period	This Call-off Contract can be extended by the Buyer for 2 periods of 12 months each, by giving the Supplier 30 days written notice before its expiry. The extension periods are subject to clauses 1.3 and 1.4 in Part B below. 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. [The extension period after 24 months should not exceed the maximum permitted under the Framework Agreement which is 2 periods of up to 12 months each. If a buyer is a central government department and the contract Term is intended to exceed 24 months, then under the Spend Controls process, prior approval must be obtained from the Government Digital Service (GDS). Further guidance: https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service

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	This Order is for the G-Cloud Services outlined below. It is acknowledged by the Parties that the volume of the G-Cloud Services utilized by Customer may vary from time to time during the course of this Call-Off Agreement, subject always to the terms of the Call-Off Agreement. This Call-Off Contract is for the provision of Services under: • Lot 3: Cloud support

G-Cloud services required	To provide agreed Maintenance, Support, requested and required innovation, and change as relates to the Legal Ombudsman Azure Environment The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below: • **Secure Managed Services on Azure**
Additional Services	**No Additional Services**
Location	The Services will be delivered at Edward House, Birmingham, B1 2RA or as instructed, or Version 1 premises, or remotely as agreed with the customer
Quality standards	**The quality standards required for this Call-Off Contract are as described in the Statement of Work (Schedule 1). Also, the quality standards required for this Call-Off Contract are as per the Supplier's G-Cloud Service Definition and UK Government best practice as defined by the Gov.UK Service Manual for the development of Digital Services**
Technical standards:	**The technical standards required for this Call-Off Contract are as described in the Statement of Work (Schedule 1). Also, Technical solutions will be delivered in line with best practice in line with Microsoft solutions on Azure, UK Government Security standards and Version 1's ISO 27001 accreditation.**

Service level agreement:

The service level and availability criteria required for this Call-Off Contract are as per the Supplier's G-Cloud Service Definition.

- The **response time** is the elapsed time from the time the call is logged and recorded in the service desk system to the time when a member of the support team carries out an initial incident triage and updates the customer.

- The **update time** is the frequency of reporting by our team to LeO users regarding progress in resolving the incident. This update would normally be via email or phone and details are added to the call record in LANDesk.

- The **resolution time** for a call is the elapsed time from the time the call is logged with the service desk to the time of resolution and/or to provide an agreed workaround until the incident is fully resolved. The "clock" will stop when the incidents is with the customer in order to get further information or carry out UAT.

The table below outlines our call categories, and associated response and update times.

Level	Description	Response Time	Update Time	Service Restoration	Target Resolution
P1	Critical Business Service or Function unavailable, severely degraded, or inaccessible	30 mins	Every 30 mins	2 hours	4 hours
P2	Critical Business Service or Function severely degraded	1 hour	1 hour / As agreed	4 hours	1 working day
P3	Non-Critical Business Service Function unavailable or degraded	2 hours	Daily / As agreed	2 working days	2 working days
P4	Non-Critical Business Service Function disrupted but workaround available	4 hours	As agreed	7 working days	7 working days
P5	A question, query, or minor bug	8 hours	As agreed	As agreed	As agreed

Our Standard Service Levels are based on prioritisation of calls and consider impact and urgency, rather than being purely based on the subjective nature of the issue. We will use the following methodologies to determine the priority of an incident. While Version 1 will understand your business and can apply prioritisations, ultimately you the customer are in a better position to know the true impact and urgency of any issue in your business. Therefore, you in LeO can escalate the priority on any incident. In return we do expect reasonable usage policy to be applied for escalations.

If an Incident has been raised by the Customer to the Service Desk and at any stage during the resolution of

this incident it needs to be re-assigned to Daisy to assist from an infrastructure perspective, the Version 1 “SLA clock” will stop. This is until the required work is completed by Daisy and the incident is re-assigned back to Version 1. The clock will then continue until the incident is fully resolved by Version 1.

Version 1 service desk provided 07:00 to 19:00 Monday to Friday (excluding bank holidays). Fully monitored 24*7 service available for P1 incidents.

The tables below are used by our consultants to assign a priority to an incident.

1. The impact AND urgency of the incident is established with the customer.
2. Based on the impact and urgency values a priority of the incident is assigned.
3. LeO can escalate the priority of any incident (reasonable use policy applies).

Table A: is used to identify the impact and urgency of an incident.

Impact	**Urgency**
1. Major - Critical Business Service or Function unavailable or inaccessible **2.** Significant - Critical Business Service or Function severely degraded **3.** High - Non-Critical Business Service or Function unavailable or degraded **4.** Moderate - Non-Critical Business Service or Function disrupted, but workaround available **5.** Minor - Question, query, or minor bug	**1.** Critical - Immediate fix required **2.** Urgent **3.** High **4.** Medium **5.** Low – Next scheduled release

Table B: Is used to establish the incident priority based on the impact and urgency values.

	Impact					
Urgency	**Priority Levels**	**1**	**2**	**3**	**4**	**5**
	1	1	1	2	2	4
	2	1	2	3	3	4
	3	2	2	3	4	4
	4	3	3	3	4	5
	5	4	4	4	5	5

Onboarding	An onboarding plan for this Call-Off Contract is not required

[REDACTED]

Collaboration agreement	Not required
Limit on Parties' liability	The annual total liability of either Party for all Property defaults will not exceed 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term 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). The annual total liability for all other 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).
Insurance	The insurance(s) required will be: ● 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. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law). employers' liability insurance with a minimum limit of £5,000,000 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 30 consecutive days.
Audit	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. Framework Agreement Clause 7.4
Buyer's responsibilities	• The Buyer will be responsible for the procurement of all software license requirements associated with this contract and associated service • Support incidents are raised with sufficient level of detail to allow initiation of the resolution process. This includes a reasonable assessment of the impact and urgency of the incident. Reasonable requests for further information from The Buyer will be responded to in a timely manner. (< 3 days). • The Buyer will review and sign-off on design deliverables in a timely fashion prior to commencement of the development phase • User Acceptance Testing to commence within 3 days of a UAT release been made available. • The Buyer to execute the UAT plan and accurately record and communicate any bugs or issues that may arise • Any Fixed price assumes Project Deliverables will be delivered as a continuous project, and that both parties will use reasonable endeavours to ensure each Project Deliverable will be completed as soon as is practical.
Buyer's equipment	Not Required

Supplier's information

Subcontractors or partners	None

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 Transfer.
Payment profile	The payment profile for this Call-Off Contract is: • Quarterly in advance for Managed Service Provision on a fixed price basis and in line with agreed rate card • monthly in arrears based on services delivered on a Time and Materials basis and in line with agreed rate card.
Invoice details	The Supplier will issue electronic invoices Quarterly in advance for Managed Service Provision and Monthly in arrears for Development Services. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.
Who and where to send invoices to	[REDACTED]
Invoice information required	All invoices must include a valid PO Number and full details of the service provided.
Invoice frequency	The invoice will be sent to the buyer Quarterly in advance for Managed Service Provision and Monthly in arrears for Development Services.

Call-Off Contract value	The total value of this Call-Off Contract is £1,645,461.90 (ex VAT)
Call-Off Contract charges	A breakdown of the call-off contract charges is illustrated below [REDACTED] *note the above running costs are max figures including azure hosting, the customer will only be invoiced based off actual usage figures

Additional Buyer terms

Performance of the Service and Deliverables	Service Performance is calculated by attributing points to each ticket raised in the categories of P2 to P4 *Example scenario:* A minimum of 20 calls must be raised per month for this to apply. There were 50 tickets raised in this scenario month. Each category of ticket, P2 through to P4 has points associated as shown in the points per call column of the table below. [REDACTED] For each ticket successfully achieved within the agreed SLA timeframe the points are "gained" by the MSP. In the scenario there is a total of 145 points available in the month and the MSP has "gained" 127 points. Therefore, the calculation is as follows:

$$\frac{\text{PPmmmmmmmmm gggmmmmmgg}}{\text{PPmmmmmmmmm mmmmmmmmaaaa}} = \frac{127}{145} = 87.59\%$$

Using the service credit regime table below, the percentage falls into the 4% category, meaning the failure would attract a service credit of 4% the month's entire service cost.

[REDACTED]

On top of this we will continue with:

- Monthly Service Review Meeting.
- Monthly Invoice Review Meeting.
- Quarterly Strategic Service review
- Technical Assurance Panel

Provision of Reports, Proposals and Feedback

The Customer wishes to have a regime in which the MSP must deliver required reports and feedback by agreed dates – in some cases by a set number of working days and in other cases by a specifically and mutually agreed date to reflect complexity, scale or priority.

Service credits of 1% will be applied for any failure to submit a major incident report to The Customer within five working days of the customer (The Customer) accepted resolution of the incident, or within two working days for a security incident. This charge will apply to the month's entire service cost. If there are multiple late reports each will attract its own service credits.

Failure to send any monthly or quarterly performance reports within 5 working days of a month or quarter end (respectively) will attract a service credit of 1% of the month's entire service cost. Each late report will attract its own service credit.

Failure to provide quality assurance of The Customer developed functionality within five working days (or by an alternative mutually agreed and documented delivery date) will attract a service credit of 1% of the month's entire service cost. Each late QA assessment will attract its own credit.

Similarly, failure to supply a requested impact assessment, solution options and recommendations, or effort

	estimations for a change by the mutually agreed and documented delivery date will attract a service credit of 1% of the month's entire service cost. If there are multiple late returns each will attract its own service credits. *Service Credit Limits* The service credits payable by MSP shall never exceed (in any month) 20% of the month's entire service cost. *Changes and Service Credits* The service credit regime only applies to the core support service. Changes will be raised and costed separately on an ad-hoc basis. Failure to meet the agreed timescales for delivery of the specified scope may result in the withholding of or reduction in payments.
Guarantee	Not Used
Warranties, representations	Not Used
Supplemental requirements in addition to the Call-Off terms	Not Used
Alternative clauses	Not Used

Buyer specific amendments to/refinements of the Call-Off Contract terms	Not Used
Public Services Network (PSN)	Not Used
Personal Data and Data Subjects	Will Schedule 7 – Processing, Personal Data and Data Subjects be used – Yes

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	Version 1	Ministry of Justice on Behalf of The Office for Legal Complaints, operating The Legal Ombudsman
Title	[REDACTED]	[REDACTED]
Signature	[REDACTED]	[REDACTED]
Date	[REDACTED]	[REDACTED]

Schedule 1: Services

INTRODUCTION

- This Call Off Schedule specifies the:
  - Services to be provided under this Call Off Contract, in Annex 1.

ANNEX 1: THE SERVICES

REQUIREMENTS AS PUBLISHED IN THE INVITATION TO TENDER

- ## About the Legal Ombudsman

  The Legal Ombudsman (The Customer) for England and Wales was set up by the Office for Legal Complaints (our Board) under the Legal Services Act 2007. We receive complaints from consumers about legal services and claims management companies and address them through informal resolution and ombudsman decisions. The organisation has about 230 staff and is based in Birmingham.

- # Background to Service

  Our mission is to transform our IT landscape into a sustainable one that enables The Customer to become a more efficient and continuously improving organisation.

  We are seeking an Infrastructure managed service provider (MSP) that continues to provide a flexible and responsive service. The successful provider is likely to be characterised by a transparent approach, providing visibility to The Customer of ongoing and planned activities, running projects using a defined programme and project methodology and following acknowledged IT good practice, including ITIL.

The Customer currently has a mixture of third party and cloud hosted services across a range of suppliers providing relatively small aspects of its whole service underpinned by its current Infrastructure supplier and a single supplier providing SaaS for its Case Management System.

The Customer is seeking Microsoft Gold Partner status for its future MSP, and one who has a proven background in helping its clients to achieve service excellence through support and development of an infrastructure service integrated with its existing Case Management System ("CMS", based on CRM Dynamics Online) as well as other services in an Office 365 environment. The MSP's track record will also be strong in terms of service management excellence. The Customer would like to develop the relationship into a genuine collaborative partnership with both itself, its CMS MSP, and its new MSP – as we see this as vital to ensuring a stable and forward-looking IT service that can add real value to the business.

Our Requirements

Overview

The MSP will be a Microsoft Gold Partner which includes:

- ITIL-aligned helpdesk
- Networking and security
- Back up
- AD and exchange management
- Availability and capacity management
- Problem management
- Infrastructure updates
- Monitoring services
- Software licensing
- Service desk provision (including portal and metrics)
- Major incident management
- Service delivery management
- Managed builds for software and hardware
- Security and connectivity
- Managed switches, routers and firewalls
- Enterprise management tools
- Cloud management

- Housekeeping
- Resilience, continuity, and disaster recovery

To ensure business continuity The Customer require a full UK or EU/EEA based ITIL-aligned service management solution from a supplier with the skills, knowledge, and capacity to be able to provide both support and development to The Customer during our standard working hours (07:30 to 19:00 Monday-Friday, excluding bank holidays in England and Wales).

• Ways of working

The supplier will provide visibility of processes being followed and its adherence to those processes, including progress against KPIs. The supplier will also align with The Customer's IT governance structure as described in 3.4.12 below. The supplier will combine flexibility and responsiveness with adherence to industry good practice, including ITIL approaches to Service Management and ISO27001 compliance for security requirements. The Customer will expect regular communication from the supplier to ensure that its users are provided with a good service, it is able to manage its own resources effectively, and progress in project and incident delivery is transparent.

The Customer may require representation at its Birmingham offices on occasion but will not normally require a regular weekly presence. However, we recognise that during key periods, such as transition, there is likely to be an advantage to increased onsite presence.

• Infrastructure Management

The successful MSP will provide a robust and good practice approach to managing the infrastructure.

• Networking and Security

The network connectivity infrastructure, including the connectivity to The Customer's CMS Managed Service Provider, should be based on enterprise class design to provide a next generation zero service loss architecture, which is properly managed and maintained.

The current supplier is providing an MPLS connection from The Customer offices to its own data centres. The Customer requires the MSP to provide similar MPLS functionality or a compatible alternative solution for connections to any MSP data centres.

Secure access to and from The Customer systems and data must be through industry-leading vendor firewalls, providing high resilience and performance for the service. Physical firewalls for increased levels of segregation and security should be implemented if the design requires them and to ensure further appropriate segregation. In addition, segregation between production and non-production environments should be in place.

Where remote access is required for third party support services, two-factor authenticated remote access via the internet should be provided to administer the server infrastructure using secure point to point access.

The Customer will arrange for independent security tests to be conducted on its systems and services. These will take place at least annually but may also be required as a result of a major change. The MSP is expected to cooperate with The Customer's testing provider before and during the testing, and to develop and follow through with an action plan to address agreed priority shortcomings at no extra cost to The Customer.

The MSP must have ISO27001 accreditation, and assist with the management of The Customer's data, on the clear understanding that it will be classified at mostly "official" and in some cases "official – sensitive" level.

- ### Backup

A backup infrastructure should utilise the current industry-leading technology and be built using a progressive incremental strategy to provide an enterprise-class solution. This should ensure that new applications, operating systems and databases will be supported on release, without the need to undertake changes to the back-end infrastructure in the future. Backup retention policies will need to be defined within the contract to align to The Customer backup and retention policies.

The MSP will be required to undertake an appropriately scaled quarterly test of the backup and submit a report at the following operational service review meeting.

- ### AD and Exchange

The MSP will be responsible for the setup, upgrade and maintenance of Active Directory and our email system (Exchange). The MSP will support The Customer in making changes to cover day to day activity such as managing user account, password resets, user permissions etc.

The Customer requires all incoming and outgoing email communication to be archived in court ready format. We are currently using Webroot email archiving solution and we will require the MSP to continue supporting this solution or implement a similar compatible alternative solution if required.

- ### Availability and Capacity Management

The proposed infrastructure support approach should utilise industry standard enterprise-class availability and capacity management tools to define, analyse, plan, measure and improve all aspects of the availability and capacity of ICT services in accordance with agreed service levels and availability and capacity requirements.

The MSP must utilise appropriate tools to monitor the live environment, applying thresholds and automated alerting wherever of value.

The monitoring system should store data for historical capacity, fault and report analysis, enabling the MSP to provide trend analysis reports. Trend analysis must be used to ensure

that the whole infrastructure capacity meets current and future business requirements in a cost-effective manner.

- ### Problem Management

The MSP should utilise problem management processes that include diagnostic activities to identify root causes, and to determine the resolution to those problems. It is also responsible for ensuring that the resolution is implemented through the appropriate control procedures, especially change management and release management.

The problem management process should maintain information about problems and the appropriate workarounds and resolutions in a knowledge base, so that the MSP is able to reduce the number and impact of associated incidents over time.

- ### Infrastructure Updates

Where there are any infrastructure updates, including for virtual hardware or software, which may potentially affect The Customer's services or systems The Customer should be warned as soon as the MSP is aware. The MSP must provide a plan of works, timeframe, reason for the change, and a contingency/rollback plan. An ITIL-aligned change procedure should be followed and where disruption is inevitable or likely all work should take place out of hours, including over a weekend. All patches and updates to the infrastructure should follow a strict change control process and patches tested before application to the production servers. Application should take place to all environments, finishing with production.

• Service Management

The Customer requires the MSP to provide full management of the systems and environment deployed on premise and in Azure. The Customer requires an experienced and certified operation team to support, monitor and carry out specific tasks to ensure that the SLAs documented within the contract are met, and a strong client-centric account management function to support the good governance of the contract and services.

The Customer currently has its intranet on SharePoint 2007, which is hosted by the current supplier and managed by its third party subcontractor. The Customer is currently in the process of moving the intranet to SharePoint 2013 Online and expect this to be completed by Quarter 3 of 2017. Therefore we will require the supplier to have experience of the management of SharePoint 2007 and SharePoint 2013 online including setup and integration.

- ### Continued MSP, Development and Exit Plan

The MSP must provide a comprehensive transition project plan for the take on of the service that will ensure a seamless migration from the existing MSP whilst providing continuous and ongoing services and support with no break or disruption to The Customer's daily work activity. The transition plan should ensure that it covers the end to end service from the user desktop systems and applications through to external facing systems (such as the the Customer internet presence) and the ICT back end infrastructure.

The Customer's current Infrastructure MSP is willing to work closely with any new MSP, and similarly our CMS MSP is also lined up to support a smooth transition. The Customer requires that any new MSP work closely and constructively with The Customer's current MSPs and other suppliers. The Customer expects an outline (comprehensive but not detailed) plan as part of the initial submission, with a more detailed plan to be prepared following selection of the preferred supplier.

The MSP must also provide an outline exit plan covering all those elements that would need to be undertaken upon completion of the contract, with a clear indication of the likely duration for its fulfilment.

Note that all costs of take-on/transition and exit must be explicitly stated in the financial proposal.

- ### Monitoring Services

The Customer requires the MSP to have server/resources monitoring in place to proactively monitor on a 24/7/365 basis, preventing downtime by being able to take actions before it becomes critical. If possible, we would also like to have access to a digital dashboard showing real time information of monitored equipment and event triggers.

- ### Software Asset Management

The Customer requires that the MSP support it in ensuring that it remains compliant in regard to licencing and/or subscriptions for all components of the Infrastructure Service. The Customer requires that the MSP supports licensing across the Microsoft EA and those required for services from other third-party suppliers. The Customer expects the MSP to maintain a software asset register and, where necessary, get involved in additional licence procurement and/or subscription management.

Note that The Customer expects the MSP to have its own licences for the software it requires for both development and service management.

- ### Service Desk Provision

The Customer requires the MSP to provide an ITIL-aligned service desk supported by a service management tool. The service management tool should incorporate a Configuration Management Database (CMDB) and the Forward Schedule of Change (FSC).

The service desk should operate key ITIL-based processes including incident management, problem management, change management, service level management, release management and configuration management. All the MSP's staff, including those on the service desk, must be familiar with and operate according to its information security management regime, and with full regard to relevant legislation (including data protection).

- ### Service Desk Function

The Customer expects the service desk to triage and manage all The Customer's calls routed through The Customer's own service desk, whether raised by telephone, via e- mail,

or logged on the portal. The MSP is expected to manage, own and coordinate the resolution of any calls that require the involvement of third parties including any liaison with The Customer's suppliers and MSPs.

The service desk must be available to log and start acting on incidents between the hours on 07:30 and 19:00 Mondays to Fridays (excluding English and Welsh public holidays). There should also be emergency out of hours support to handle any major (P1) incidents that are either reported by The Customer or arise from the MSP's monitoring, with the intent of restoring normal service as soon as possible.

- ## Service Desk Portal

There must be a self-service portal front end to the service management tool that allows new calls, service requests and changes to be logged by The Customer's IT staff, plus provide additional information, track the status of open calls, and close calls.

The Service Desk should maintain a knowledge base so any repetitive issues and their solutions are quickly highlighted and able to be actioned.

Service Desk Metrics

The MSP must put in place a reporting regime that enables the production of monthly metrics related to the performance of the service desk in responding to and resolving calls/tickets. The regime should also support quarterly trend reports. For them to be of use reports are expected to have an accompanying narrative.

Major Incident (P1) Management

The Customer requires that the MSP have a robust documented approach to managing major incidents (all priority one incidents, including security breaches). The approach must involve the proper logging of the incident and all subsequent actions, whether diagnostics, provision of updates to The Customer, liaison with third parties, tests, and actions taken towards resolution. The approach must enable the MSP to produce a major incident report that covers the schedule of events, the identified root cause(s), the resolution(s) taken, and any further actions that might be pursued to reduce the likelihood of further occurrences. The Customer expects reports to be completed and supplied to its nominated contact within five working days of the incident's resolution. All reports within the month must be placed on the agenda for discussion at the following month's service review.

- ## Service Delivery Manager

As part of the service delivery management mechanism, a Service Delivery Manager (SDM) should be appointed and should liaise with both the Service Delivery Manager of The Customer's CMS Managed Service Provider and The Customer's nominated contacts. The SDM should be the single point of contact for all service delivery issues, liaising with its own internal departments to ensure that service level agreements are met within agreed criteria, and meeting with The Customer representatives to ensure that services are delivering to expectation.

The SDM should operationally manage the provision of all contracted services and ensure any issues are dealt with in a timely and professional manner. The role should coordinate

the involvement of other MSP staff involved in delivering the day to day service, and liaising with any designated person(s) responsible for coordinating the delivery of non BAU (business as usual) change.

- ### Account Management and Direction

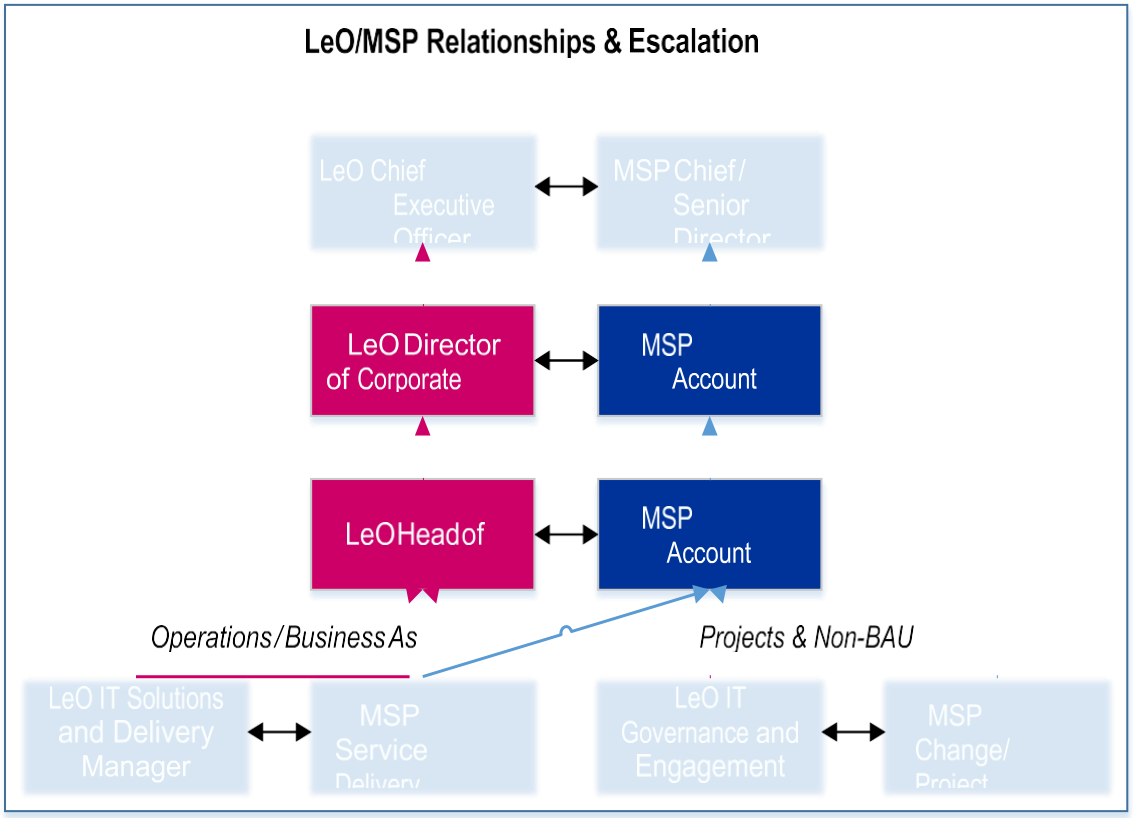
The Customer requires the provision of a named account manager who will provide a point of escalation for the Head of IT. The account manager will be senior to and have authority over both the service delivery manager and any person given responsibility for coordinating non-BAU change.

The Customer also requires the designation of a named account director, who will be senior to and have authority over the account manager, to provide a further point of escalation for The Customer's Director of Corporate Services.

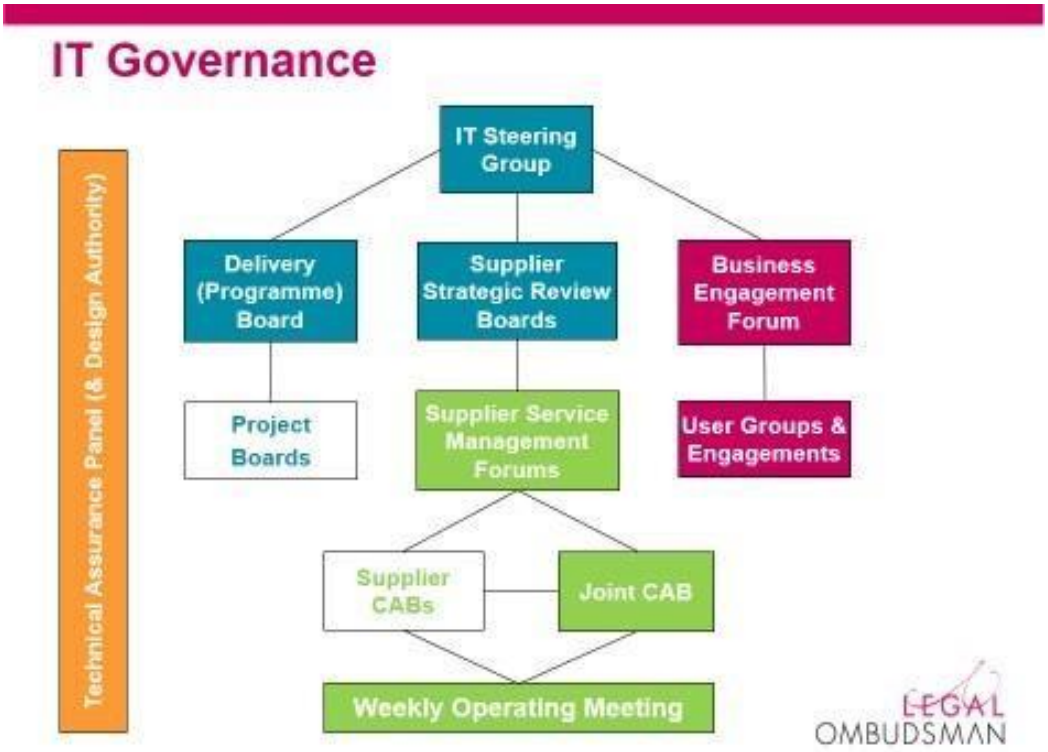
- ### Escalation Routes

In case of issues that cannot be resolved at lower levels, The Customer requires that the MSP has a documented escalation process with clear routes to progress issues. The Customer would wish to ensure that counterparts at various levels in the chain have the opportunity to develop and build stable peer relationships to facilitate timely and helpful action in the event of an issue arising in either organisation.

Although The Customer anticipates that the following general structure would be needed to support this contract, this clearly does not preclude the involvement of other personnel as required by either party to deliver their obligations.
On a day-to-day basis The Customer supplier management will be led by our IT Delivery and Operations Manager, Irfan Faruki. A number of his team will be involved in liaison on issues and/or projects.



- Service Reporting and Reviews



The graphic above shows the current IT governance structures operating in The Customer. These may be subject to some amendment to align with a The Customer modernisation programme that is underway.

The MSP will be required to provide appropriate representation to The Customer's quarterly Supplier Strategic Review Boards and monthly Supplier Service Management Forums. The MSP must also provide appropriate technical expertise in writing for consideration by The Customer's own Change Advisory Board or that organised by The Customer's CMS MSP. Representation may also be required by the technical assurance panel or any Delivery Board (excluding closed agenda items) in writing or by telephone.

The Supplier Strategic Review Board is designed to enable senior management at The Customer to engage appropriately with senior management from its major suppliers. The purpose of the Supplier Strategic Review Board is to ensure that:

- strategic issues and information are shared by both parties
- escalated issues are resolved expediently and effectively
- a culture of partnership is developed and maintained
- service and contract performance is subject to high level review

The Supplier Service Management Forum is designed to facilitate good working relationships, clarity of purpose and financial control between The Customer and its MSPs. The purpose of the Supplier Service Management Forum is to:

- review the supplier's performance report for the last period
- agree any service credits that may be due
- discuss incident reports and any proposed preventative measures
  - discuss progress on problems and items in the Continuous Service Improvement Plan (CSIP)
  - escalate issues that cannot be resolved within the forum to either senior individuals from The Customer and the supplier or the SSRB
- note any significant business matters that may impact on service
- review the arrangements for changes being accepted into service

The functions of the Technical Assurance Panel are to:

- review all new IT change proposals to ensure they are sufficiently complete to be able to identify potential solutions
- Identify and raise any technical implications of potential solutions for changes (e.g. to functionality, new system constraints, security concerns, etc.)
- help IT management to recommend the rejection or approval of a change based on its technical feasibility and merits
- bundle any technically related changes into more substantial packages

The functions of Delivery Boards are to oversee the delivery of significant The Customer IT projects or programmes.

- ### Continuous Improvement

The Customer welcomes an MSP who wishes to show true partnership and help us to improve all aspects of the solution and the associated service in order to create efficiencies and derive better business value from our investment.

The Customer wishes to move to an integrated and coherent infrastructure, whilst relying on a smaller range of suppliers - but doing so in a managed, clear manner that reduces risk rather than increasing it.

The Customer anticipates allocating a number of call off days on an annual or monthly basis to enable the implementation of minor enhancements to the service.

• Managed Infrastructure Service

The Customer requires the MSP to provide 24/7/365 management of the environment, including proactive monitoring, root cause analysis, capacity/availability monitoring, management, and reporting.

The MSP must have the expertise and operational experience in monitoring and managing servers and services in Azure environments, including Microsoft servers (Windows Server, SQL Server, Active Directory/LDAP, Exchange, Skype, SCCM, SharePoint and Dynamics CRM, etc.).

The MSP will also be responsible for setup and maintenance of the email system, web proxy, DNS, backups, account management, software patches upgrade, performance tuning, storage allocation, system maintenance, network monitoring and troubleshooting, network management, maintenance, and monitoring of systems for high availability and reliability.

The MSP will design, setup, support and troubleshoot the full network infrastructure system (including LAN, WAN, secured WIFI service and access points, VPNs, internet connectivity, firewalls, etc.).

The MSP will create and maintain a full network topology diagram in accordance with industry standard practice. The MSP must also have a documented approach to keeping the software and environments current and up to date in respect of versions and patching, etc.

- ### Managed builds for software and hardware

The Customer is currently in the process of moving to a mixed estate of desktops and laptops for its end user devices. These machines will be running a mixture of Windows 10 and Windows 7 OS – although The Customer wishes to converge on one OS over time. The MSP will be required to build and maintain corporate desktop images in line with industry good practice that will efficiently install on any corporate-supported hardware and will provide the desktop, applications and customisations they need in order to perform their jobs.

The Customer would like the MSP to continue to advise it on its end user device replacement and deployment strategy so that it remains in line with industry standards and good practice.

- Security and Connectivity

The Customer is currently accredited to ISO27001 but is exploring alternative approaches. The MSP will be required to support any regime in place.

The MSP is required to conduct its own annual penetration tests (in addition to those described in 3.3.1) using an independent supplier and to carry out necessary remedial work as per penetration test results.

The MSP will also be responsible for appropriate hardening within our network, between our network and the MSP's, and our connection(s) to the Internet.

The MSP will be required to support any security or connectivity activity resulting from any changes to the The Customer estate.

The MSP will be required to support secure remote access by The Customer staff. This is currently managed by the use of Signify tokens, but The Customer is open to alternative approaches that incorporate 2FA.

- Managed Switches, Routers and Firewalls

The Customer requires the MSP to provide 24/7/365 management of the CISCO switches, CISCO routers, Juniper VPN connectivity, and Barracuda firewall deployed within the Azure environment.

- Enterprise Management Tools

The MSP is required to deploy enterprise-class management tools for monitoring, deployment, and configuration management, and to provide service automation where appropriate.

Monitoring information should be presented as a real-time topology, with application and component-specific alerts directed to The Customer and, if required, other nominated third parties. The monitoring system should store data for historical capacity, fault and report analysis, enabling the MSP to provide trend analysis reports.

Reports from the tools used for deployment, configuration management and service automation should be provided by exception in the event of a significant error, but otherwise retained for historic trend analysis and fault diagnostics.

- Cloud Management

The Customer is moving toward using Azure IAAS. Therefore, the MSP will be required to carry out Windows Azure cloud administration, including establishing the infrastructure,

monitoring, troubleshooting, server management and maintenance, and migration of on-premise servers to Azure.

- ### Telephony over the Infrastructure

The Customer is not looking for the Potential Providers to provide telephony; however, The Customer runs VoIP (Cisco Jabber and RedBox voice recording) and intends to move to a cloud hosted telephony solution during 2017. The MSP will be required to support continued integration of the existing telephony solution, and to design the necessary infrastructure and help facilitate the required change.

The Customer wishes to replace its existing IM and telephone solution with a unified communications solution that integrates well with its Microsoft based environment and offers features including presence, IM, voice (and possibly video) calls, incoming and outgoing call recording, online meetings for The Customer users, as well as integration with Exchange/Outlook and CRM Dynamics. Skype is currently being used in a limited capacity for audio conferences and as such will be considered as part of the future unified communications solution.

- ### Housekeeping

Regular housekeeping exercises should be undertaken to ensure that The Customer's storage space and data files are free of unnecessary log files, white space and other system and monitoring files not relevant to The Customer's business or reporting. Any log files that may prove useful in the event of a major incident must be retained within the MSP's own infrastructure for at least three months – and longer if necessary.

- ### Resilience, Continuity, and Disaster Recovery

The MSP is required to advise upon and were agreed to undertake any work on The Customer's infrastructure to ensure that our business critical services are resilient and configured to provide high availability (over 98% availability, preferably over 99% in working hours). Critical components should be designed, deployed and implemented to remove single points of failure.

The Customer requires that the MSP maintain its own organisational business continuity plan and appropriate disaster recovery provisions to ensure continuity of its own support services and associated operations.

The Customer also requires that the MSP provide and manage appropriate disaster recovery services within the Azure and MS Online configuration and for all aspects of The Customer's wider IT infrastructure, including undertaking appropriate liaison with our CMS MSP. An appropriate annual DR rehearsal exercise, including planning, documentation, execution and post-rehearsal remediation of results, must be carried out by the MSP.

• Continuous Improvement

The Customer is currently using services from various suppliers together with its Infrastructure MSP. It is seeking to move to a more integrated set of services including hosted telephony, resilience improvements, new standard desktop build, and virtual desktop, single sign on. It is also seeking to move to a more cloud-based estate using an IaaS and SaaS approach.

The MSP is required to work with The Customer to develop a roadmap to modernise, streamline, and strengthen the infrastructure and associated services.

• Managing Change

The MSP must ensure that it has in place documented good practice for managing infrastructure changes and responding to changes in the wider application estate.

The MSP must ensure that standard methods and procedures are used for efficient and prompt handling of all changes to control ICT infrastructure in order to minimise the number and impact of any related incidents upon service.

• Expertise and Third-Party Relationship Management

The MSP must be a Microsoft Gold Partner with strong expertise in Office 365 and Azure services.

The Customer would prefer that the MSP did not use any further subcontractors but acknowledges that for the purposes of capacity and capability it may be necessary from time to time to subcontract highly specialised services with the agreement of The Customer. The Customer requires that the MSP takes full responsibility for any subcontractors it needs to use and manages them accordingly with appropriate operational level agreements (OLAs) that support The Customer's required service levels. Similarly, the MSP must ensure that it has agreed escalation paths with its subcontractors should there be any issues with delivering to meet expectations and requirements. The MSP will be held solely accountable for the performance of its subcontractors, specifically for any failings that impact on The Customer.

• Change/Project Governance and Process

The MSP must provide a weekly progress report on any active changes; these must include traffic light statuses for each change against their baseline agreed timescale.

For new projects or major changes, the MSP must take a recognised project management approach (preferably based on PRINCE2) to ensure that standard methods and procedures are used to deliver the project within agreed timescales, within budget and to specification. It is essential that the MSP advocates strongly for quality to be balanced with cost and time, and that it provides early comment on any apparent scope creep.

For new planned works, changes or projects, the MSP must plan for and deliver against a Forward Schedule of Change that is aligned to The Customer's own. The schedule must include any upgrades to Microsoft online services and to any add-ins, so that the entire solution remains no more than one full version behind the latest available.

Likewise, the MSP must proactively maintain any firmware and software relating to the infrastructure, providing advice that helps The Customer to move towards a position where all such items are as up to date as pragmatically possible.

The MSP's change process must include engagement and communications from requirement through to deployment. It must also be capable of scaling to handle both small/simple and large/complex work packages. It must also include sign off "gates" with specified acceptance criteria (to include any required documentation).

The Customer requires that the MSP ensures that the process incorporates formal mechanisms to check on business readiness and the readiness of all those involved in technical support. This may require contributing to end user documentation and training plans, and authoring technical support notes and providing training to technical staff.

- ### Requirements and Options

The Customer will provide high level requirements specifications that do not necessarily indicate a specific solution, but we may suggest one. The Customer expects the MSP to take the lead on identifying the range of potential solutions, and the MSP should feel at liberty to counter any expressed preferences with an appropriately reasonable argument. The Customer expects the MSP to take into account our IT governance principles (Appendix 2) in considering potential solutions.

The MSP will be required to conduct both requirements and design workshops, involving the appropriate The Customer personnel, and is expected to provide constructive challenge to both The Customer business users and IT staff. The outcomes of these workshops must result in appropriately detailed specifications and design options, and as such the MSP must require clarifications from The Customer and not make assumptions (or at least specify any working assumptions that need clarification).

The Customer requires that the MSP provide options analyses and recommendations in response to RFCs or The Customer senior management requests. We expect to receive these as documented proposals that includes costs and effort/duration estimates for all options, but with greater specificity for recommended options.

- ### Testing and Assurance

The MSP is expected to conduct unit and systems (including regression) testing before handing over to UAT, and automated test tools should be used where appropriate. Significant faults must be fixed prior to passing into user acceptance testing.

The Customer requires the MSP to use appropriate tools to log and track defects/bugs (and their subsequent fixes) that arise from testing.

The Customer wishes to be able to undertake its own changes wherever it has the capability and capacity to do so. This will require the MSP to agree with The Customer a set of processes that are appropriate for different sorts of changes – some of which will be light touch and others of which may require fuller assurance. The overriding factor is to manage any risk to the integrity of the system, whichever environment the changes are being made to. The Customer requires that the maximum period for providing such assurance is five working days after the request has been submitted.

- ### Environments and Deployment

The Customer requires the MSP to develop installation plans for changes, and that all plans should incorporate rollback and/or other contingency measures.

For every change the MSP should follow an ITIL-aligned release management process. The process should be designed to plan, schedule and control the movement of releases to test and live environments. Release notes must be prepared for every new release, and functional and technical design documentation must be prepared or updated, as appropriate.

• Proposed Service Levels

The Customer wishes to have a structured set of service levels that can be used to monitor application service performance and provide a service credit regime to compensate The Customer for failures. The Customer is proposing the following approach, as set out in the subsections below. However, we expect to discuss this with supplier of the best fit solution, which may identify a better alternative. Given our partnership ethos, we would particularly encourage proposals for incentive-focused schemes.

Priority Definitions

	Impact		
	H	M	L
Urgency H	1	2	3
Urgency M	2	3	4

The Customer's prioritisation is based on impact to its business and urgency as shown in the diagram to the left

	Description
P1 - Critical	Complete loss of connectivity and/or service (including significant functionality or component) for all its users
P2 – High	Loss of connectivity and/or service for some of its users
P3 - Medium	Problem or fault which has a minor impact on service but is not business critical
P4 - Low	Problem or fault which has no impact on service but requires resolution, and RFIs (requests for information)
P5 - Very Low	Service request which should have no impact on service but requires implementation

Priority Code	Description	Target Response Time	Service Restoration	Target Full Resolution Time
1	Critical	30 minutes	2 hours	4 hours
2	High	1 hour	4 hours	1 working day
3	Medium	2 hours	2 working days	2 working days
4	Low	4 hours	7 working days	7 working days
5	Very Low	8 hours	As agreed	As agreed

- ## Major Incident Reports

All P1 incidents shall require a major incident report (MIR) to be produced by the MSP within 5 working days of its resolution, and within 2 working days in the case of a security incident. These reports must include information on the identification, diagnostics and other actions, description of symptoms and root cause, resolution, and recommendations for further action to reduce the likelihood of recurrence. MIRs shall be reviewed at the next possible operational service review meeting.

- ## Service Credit Regime

The Customer wishes to have a service credit regime that is based on availability, service performance, and reporting. To facilitate the availability aspect of this regime it will be necessary to divide the entire service into individual service lines

- ### Availability (P1)

Application availability is based upon access to the service being in line with the definition associated with the P1. P1s are only used to record outage and availability issues.

Any agreed downtime is excluded from the calculation of any service credits.

Example Scenario:

The month of November has 30 days, i.e. 720 hours or 43200 minutes.

If an agreed P1 lasts for 90 minutes in the month, this would mean that the system was only available for 43110 minutes (43200 – 90). Therefore, the calculation is as follows:

$$\frac{43110}{43200} = 99.79\%$$

Using the service credit regime in the following table, this would attract a 10% service credit against the line for the specific service impacted.

Availability Achieved	Applicable Service Credit
99.99% to 100%	0% of the Monthly Charge of the Service Line
99.8% to 99.989%	5% of the Monthly Charge of the Service Line
99.5% to 99.799%	10% of the Monthly Charge of the Service Line
99% to 99.499%	20% of the Monthly Charge of the Service Line
Less than 99%	40% of the Monthly Charge of the Service Line

- Service Performance (P2-P4)

Service Performance is calculated by attributing points to each ticket raised in the categories of P2 to P4

Example scenario:

A minimum of 20 calls must be raised per month for this to apply. There were 50 tickets raised in this scenario month. Each category of ticket, P2 through to P4 has points associated as shown in the points per call column of the table below.

Category	Points Per Call	Calls Raised	Failed Calls	Points Available	Points Gained
P2	5	20	3	100	85
P3	2	15	1	30	28
P4	1	15	1	15	14

For each ticket successfully achieved within the agreed SLA timeframe the points are “gained” by the MSP. In the scenario there is a total of 145 points available in the month and the MSP has “gained” 127 points. Therefore, the calculation is as follows:

$$\frac{mmmmmmmmmmmmmmmmmmmmmmmmmm}{mmmmmmmmmmmm\ mmmmmmmmmmmmmmmmmmmm} = \frac{127}{145} = 87.59\%$$

Using the service credit regime table below, the percentage falls into the 4% category, meaning the failure would attract a service credit of 4% the month's entire service cost.

Lower	Upper	Credit
90.000	100.000	0%
80.000	89.999	4%
70.000	79.999	8%
0.000	69.999	16%

- ### Provision of Reports, Proposals and Feedback

The Customer wishes to have a regime in which the MSP must deliver required reports and feedback by agreed dates – in some cases by a set number of working days and in other cases by a specifically and mutually agreed date to reflect complexity, scale or priority.

Service credits of 1% will be applied for any failure to submit a major incident report to The Customer within five working days of the customer (The Customer) accepted resolution of the incident, or within two working days for a security incident. This charge will apply to the month's entire service cost. If there are multiple late reports each will attract its own service credits.

Failure to send any monthly or quarterly performance reports within 5 working days of a month or quarter end (respectively) will attract a service credit of 1% of the month's entire service cost. Each late report will attract its own service credit.

Failure to provide quality assurance of The Customer developed functionality within five working days (or by an alternative mutually agreed and documented delivery date) will attract a service credit of 1% of the month's entire service cost. Each late QA assessment will attract its own credit.

Similarly, failure to supply a requested impact assessment, solution options and recommendations, or effort estimations for a change by the mutually agreed and documented delivery date will attract a service credit of 1% of the month's entire service cost. If there are multiple late returns each will attract its own service credits.

- ### Service Credit Limits

The service credits payable by MSP shall never exceed (in any month) 56% of the month's entire service cost.

- ### Changes and Service Credits

The service credit regime only applies to the core support service. Changes will be raised and costed separately on an ad-hoc basis. Failure to meet the agreed timescales for delivery of the specified scope may result in the withholding of or reduction in payments.

The Customer Statement on Equality and Diversity

The Office for Legal Complaints serves a diverse society. That is a society made up of men and women; of people of different races, cultures and religions; of people with and without disabilities; of young people and older people; of straight and gay people; of people with and without caring responsibilities; and of people with many other differences.

We recognise, respect and value that diversity and will strive in all we do to serve the interests of people from all sections of society. We will also strive to become an organisation that reflects more fully the diversity of the society we serve and truly values the contributions which staff from all sections of society makes to our work.

In particular we:

- In the development of our policies, take account of the interests of all sections of society
- Ensure that, wherever possible, the services we provide meet the needs and expectations of all our service-users; and
- Seek to influence others with whom we work, or from whom we purchase goods and services, to share our commitment to valuing the diversity of our society

To meet our business objectives, we:

- Provide real equality of opportunity in the recruitment, development and promotion of all our staff
- Eliminate unfair discrimination and harassment in our workplace
- Extend family friendly working practices
- Develop all our staff to their full potential and make best use of their different talents
- Consult staff, including staff from minority groups, about how we can improve equality of opportunity and support diversity.

We set ourselves goals with measurable outcomes to assess our progress towards becoming a diverse organisation providing excellent service to all sections of society. We hold ourselves accountable for their achievement.

We expect our suppliers to uphold these values both as part of their normal day to day activities and in relation to their dealings with us.

The Customer Statement on Confidentiality and Non-Disclosure

The Legal Ombudsman, by advertising, and the bidder by responding to this invitation to tender agree to participate in the following joint Non-Disclosure Agreement for the purpose of information shared to enable them to exchange freely commercial and technical Confidential Information regarding the subject of this document.

Accordingly as a precondition of such exchange of information and discussions it is hereby agreed between the parties to this Agreement as follows:-

"Confidential Information" shall be any and all drawings, designs, specifications, models, samples, devices, manuals, reports, plans, diagrams, prototypes, computer programs, documentations and other things in which copyright subsists together with any and all information results, data, calculations, know-how and other things which are received by either party from the other during or as a consequence of any exchange of information or discussions, (verbally or visually transmitted information to be confirmed in writing within thirty days of its disclosure) but shall not include anything which:-

- was already properly and provably in the possession of the recipient party, or
- was already in the public knowledge at the time it was received from the other party hereto, or
- subsequently becomes public knowledge through no default on the part of the recipient party, or
- is received from a third party having good legal title thereto and not under any obligation of confidentiality, or
- is independently acquired by the recipient party as a result of work carried out by or for the recipient party by personnel to whom no disclosure of the relevant Confidential Information has been made.

Each party hereto shall keep confidential all Confidential Information it receives from the other party. In particular it will not disseminate any such Confidential Information amongst its employees except to the extent strictly necessary to perform any evaluation agreed by the other party during or as a consequence of the discussions and it will use its best endeavours to ensure that none of its employees copies, discloses or uses Confidential Information except as hereby permitted; in this connection (but without limitation) each party will use at least the same degree of care in safeguarding Confidential Information of the other party as it uses in safeguarding its own information of a similar nature.

Each party shall use Confidential Information received from the other party solely for the purpose of evaluations agreed during or as a consequence of the discussions and shall return all of the other party's Confidential Information in material form on request by that other party.

The restrictions and obligations imposed hereby shall continue in force for five years after the effective date of this Agreement save that the provision of clause 2 shall continue to apply to each item of Confidential Information for a period of five years from its disclosure.

Nothing in this agreement shall be deemed to create a partnership or agency between the parties, or to grant or convey any licence (express or implied) under, or right to, any intellectual property comprised in Confidential Information disclosed hereunder.

Each party will be solely responsible for making its own judgement and decision on all Confidential Information. Neither party makes a representation or warranty as to the accuracy or completeness of the Confidential Information.

Each party confirms that in relation to the purpose set out above, it is acting as principal, and not as agent for or in concert with any other person.

It is understood that the obligations contained herein shall be binding on the successors, employees and representatives of both parties.

This Agreement shall be governed under the laws of England.

For the duration of this Agreement and for one year thereafter neither party will directly or indirectly solicit or entice away from the other party any employee of the other party where that employee is or has been directly or indirectly involved in any aspect of this Agreement."

The Customer's Current Network Deployment

[REDACTED]

The Customer's IT Governance (Architecture) Principles

1. Decided by Strategy	IT investments must be able to demonstrate a clear link to and support at least one of The Customer's strategic goals
Rationale: The Customer's business and its success relies heavily on its IT, and its IT investments must therefore be focused on enabling the overall direction set by its strategy.	
Implications: ▪ The Customer will not pursue any change requests that are unable to properly articulate how they support the corporate strategy ▪ The prioritisation of change requests will take into account relative contribution to strategy execution ▪ The IT function will have a strategy (or vision) that supports The Customer's strategy and is owned by the IT Steering Group	
2. Decided for the Organisation	IT investments must take into account the wider needs of the organisation and the corporate good, and be determined centrally
Rationale: Silo approaches to IT result in duplication and overlaps, and unnecessary administration and financial overheads.	
Implications: ▪ The Customer will not tolerate the acquisition of any element of ICT (people, systems, contracts, etc.) outside of the corporate IT function without the explicit agreement of the IT Steering Group and clear support from The Customer's IT function ▪ Decisions about uncommitted IT expenditure will be the preserve of the IT Steering Group ▪ Additional solutions will not be pursued where there is an existing one that meets the primary requirements ▪ Those involved in considering change requests will need to consider the impact on all parts of the organisation, opportunities for greater synergy, and the potential for an enterprise solution ▪ All solutions in use within The Customer, including tactical and individually-created ones, belong to The Customer and may be replaced with corporate solutions at the behest of the IT Steering Group	
3. Decided by Business Case	IT investments must be supported by a robust business case that demonstrates consideration of options as well as costs and benefits
Rationale: Limited financial and human resources mean that IT investments need to be prioritised on the basis of the value they bring to the business.	
Implications: ▪ Prospective IT investments will be required to have a business case in the format determined by the IT function, and will not be put before the IT Steering Group without a sufficiently convincing one ▪ The financial case will need to reflect a comprehensive view of associated costs, both initial and ongoing, so that the total cost of ownership can be understood	
4. Designed to Serve Customers	IT solutions must take account of available customer channels and facilitate efficiency and ease of interaction with The Customer

Rationale: As a public service The Customer must be customer-centred, whether the customer is a consumer, an individual professional, or a company.

Implications:

- Process and information flow mapping will take account of customer journeys and interactions with The Customer
- The relative value and purpose of different channels will inform requirements capture, solution recommendations and subsequent detailed design
- Solution designs will seek to minimise both the number of customer touch points and the burden on customers

5. Designed for Usability	IT solutions must be designed (or selected) to facilitate ease of use and be supported by business-contextualised training and guidance

Rationale: The Customer is responsible for maximising the use of all its resources, including all its people and its IT systems.

Implications:

- Although access to IT solutions will be based on the needs of the role, reasonable adjustments will be provided where required for an individual
- Impacted end users will be represented when defining usability requirements for IT solutions and in any aspects where system features are configurable or customisation is needed
- Software and information architecture will seek to ensure as little information/data input as possible and as much as necessary to meet the organisational business needs
- Software and information architecture will provide logical navigation and intuitive, consistent user interfaces
- The business change owner has the responsibility of ensuring that in-system help functionality, written user guides, and any training are contextualised to provide real world meaning for users

6. Designed for Efficiency	IT solutions must prioritise efficiency though process simplicity, value-adding automation, and component re-use/sharing

Rationale: As a publicly funded organisation The Customer is required to continue to seek efficiencies in the way in which it conducts its business.

Implications:

- Processes/workflows will always be comprised of as few steps as is possible to meet the requirement, and incorporate automation wherever cost-effective
- Business change owners will need to critically appraise their processes and associated information flows as part of the requirements gathering process
- Solution design will always look to re-use or share existing components within a system before adding similar components that increase overheads and the risk of instability

7. Designed for Longevity	IT solutions must deliver immediate needs and ensure supportability and upgradability, whilst providing flexibility for future needs

Rationale: In seeking value for money The Customer is obliged to consider the longevity of its IT investments in accordance with its strategic direction.

Implications:

- For all IT solutions a coherent scope and purpose will be documented during requirements capture to protect against the threat of future opportunistic and less relevant add-ons that put solutions at risk
- IT solutions will avoid non-native functionality wherever possible so that they are at less risk from failure during associated upgrades; any exceptions must have a compelling rationale
- Solution design will ensure that software and hardware architecture is built to meet current needs and affordability, whilst mindful of any future extensibility (or scalability) that is articulated during requirements capture
- Wherever tactical solutions are permitted, usage limitations will be established so that they do not become critical to the business
- All plans for new IT solutions or significant changes will incorporate consideration of how they are supported both during and long after go live

8. Designed for Interoperability	IT solutions must avoid technology divergence and avoid unnecessary deviation from native functionality

Rationale: Complexity within and across IT systems has additional avoidable long term costs.

Implications:

- The Customer will maintain a common technology stack that provides for ease of interoperation, and only invest in industry standard solutions that work well with its stack
- Tight-coupling of systems will be avoided, with loose-coupling used where necessary, and interfaces will be favoured over integration
- To reduce alignment overheads The Customer's IT will have as few environments as possible and as many as necessary
- The Customer will always look to buy instead of build, and only code or complicate where an essential business need cannot be met through configuration of native functionality
- The Customer will standardise on one version of each software package, and to ensure supportability and compatibility we will aim to be no more than one version behind the latest

9. Designed to Comply	IT solutions must take account of pertinent legislation, regulations and applicable government policy

Rationale: As an arm's length body The Customer is subject to both the law and requirements impacting all government bodies.

Implications:

- The Customer will acquire its IT in accordance with government specified procurement requirements
- Information and data requirements capture will incorporate consideration of both information rights and security such that solutions are designed with both in mind
- Security architectures will be designed to be as low maintenance as possible, and take a role based approach to permissions management
- The Customer will favour government-wide frameworks and tools over commercial alternatives

10. Delivered with the Business	IT solutions will only be delivered with the active involvement of the impacted business unit(s)

Rationale: IT solutions that address a business problem are more likely to succeed with a partnership approach.	
Implications: ▪ Any IT change that does not have the ongoing active involvement of a business change owner will be put on hold ▪ Business change owners will provide sign off of requirements and process/information flow maps, identify and realise benefits, and allocate resource for user acceptance testing and training delivery; hence they will need to be senior enough to have responsibility for the associated process, information, and staff ▪ Business engagement lasts for the whole lifecycle of the solution - from identifying the requirement through to its active running and eventual decommissioning ▪ Business change owners are responsible for specifying rules and user behaviours that will ensure sufficient integrity of information, data, and metadata so that the subsequent outputs, including reports, are accurate and valid	
11. Delivered using Good Practice	IT solutions must leverage appropriate acknowledged good practice if their results are to have the requisite business longevity
Rationale: Following IT good practice is more likely to result in solutions that are delivered well and fit for purpose.	
Implications: ▪ All IT changes, projects or not, will need to be properly planned and controlled through each phase of delivery ▪ Good practice will be adapted rather than adopted so that it is proportionate to the organisation and the scale of the change, and IT will maintain documentation about its chosen practices ▪ Business change owners will need to bring IT in early to ensure that advice can be given on the achievability of any intended delivery timescales; failure to do so may result in expectations management issues ▪ There will be structured approaches to requirements capture, data/information mapping, process modelling, solution design, implementation, testing, maintenance, and decommissioning	
12.Designed for Continuity	IT solutions must facilitate business continuity by incorporating appropriate mitigation or elimination of likely risks
Rationale: The effective operation of The Customer's business is reliant on the access to its IT systems.	
Implications: ▪ Solution architecture will build in resilience and redundancy wherever justifiable and cost effective ▪ Service level agreements with IT suppliers will include availability measures to meet business requirements, but subject to affordability and achievability ▪ IT disaster recovery for solutions will be established to match The Customer's approach to business continuity ▪ Solutions will be built and maintained to minimise the likelihood of digital obsolescence in relation to its hardware, software, and its data/information	

The Customer IT Vision (Short-Medium Term)

Our mission is to transform our IT landscape into a sustainable one that enables The Customer to become a more efficient and continuously improving organisation.

1. In the future The Customer staff will no longer need to take laptops back and forth between home and office. We will enable those who wish to do so to securely connect to the corporate network from home using their own (unsupported) personal devices, but with the necessary means to securely protect our corporate data and how it is used. This will enable The Customer IT to deploy more cost effective and easily substituted equipment across much of the office.

2. We will better support those whose role requires them to work from places other than the office or home by providing lighter equipment. This may include convertible/hybrid devices for senior managers, facilitating easier paperless meetings. Board and Committee members will also be able to use the same paperless meeting facilities using their own (unsupported) personal devices.

3. Our corporate telephony and call recording systems will be improved to ensure that we have a robust enough solution to meet our business needs. It will also provide enhanced facilities for audio and video conferencing in meeting rooms, including the ability to use virtual whiteboards and save the content to our network.

4. Staff will also experience an improved and more stable case management solution, which will have been simplified to limit non-native add-ons and will increase efficiency by reducing the number of screens and clicks required. The customer experience will also be enhanced with the system enabling interactions from a wider range of digital channels, and by reducing paper-based interactions wherever possible.

5. We will invest in better business intelligence tools to enable the production and publishing of both standard and ad-hoc MI reports. This will include providing staff with easy to use tools to undertake their own analysis.

6. The Customer will have a new intranet that provides staff with vastly improved functionality, including the ability to search across its associated document store and other information repositories, and a staff directory that is maintained and updated as people join and leave. It will facilitate the easy publishing and updating of content by staff using familiar tools.

7. Similarly our website will be revamped and provisioned to enable staff to contribute draft content using familiar tools. Extranet facilities will be provided, enabling The Customer to collaborate with its partners and regulators, and our systems will also enable easier and more integrated surveys and consultations with the external audience.

8. We will support the continued professionalisation of The Customer through delivering corporate branding of backgrounds, screensavers and emails. We will provide a smaller suite of document templates that are both greener and better integrated into our systems so that staff can access them whichever way they create a new document.

9. We will further professionalise our IT function so that it can provide service in accordance with acknowledged good practice, and that we have the necessarily capabilities in house or on call to deliver what the business requires. We will provide better and more proportionate IT governance, so that processes are clearer to The Customer staff and decision making is strategic and corporate rather than tactical and frontline only.

10. IT will continue to build its relationship with all parts of The Customer and to push for a wider appreciation of the necessary business input and involvement to make IT solutions successful.

11. The Customer staff will have a self-service IT Service Desk portal, enabling them to log and track their own incidents and requests, and enabling the IT team to allocate actions internally or with our supplier(s). Staff will also be able to readily provide feedback on the team's performance, which along with other service desk metrics will be reviewed to help drive continuous improvement.

12. All single points of failure in The Customer's infrastructure will have been identified and appropriate resilience measures put in place to support business continuity. Recovery arrangements will have been updated to reflect the move to the Cloud.

13. The Customer will move towards reducing the number of IT suppliers and the associated administration and management overheads. We will ensure that suppliers take responsibility for their subcontractors and provide service levels that are backed off associated operational level agreements.

14. Although the description above avoids specific product names, for supportability and interoperability The Customer will continue to converge on a technology stack predominantly based on familiar Microsoft technologies for which we can more easily recruit skilled staff. We will also, wherever possible, maintain only one version of any product and strive to be no later than one version behind the latest available one. Within the Cloud, upgrades that often provide improved features, are usually mandatory. Maintaining compatibility of linked products is essential to our day to day working.

15. Similarly and to ensure maintainability we will standardise hardware, such that at any point in time there will be a single brand and model for each device type. We will also introduce refresh cycles that take account of the point at which the device is no longer cost effective to support.

16. We will also work with other centres of expertise around the organisation to help improve the way in which we configure and then use systems:

    a. This will include activities to develop stronger information management discipline throughout The Customer, developing taxonomies, metadata, and information architectures that meet business needs, are easy to use, and enable retrieval.

    b. We will also work more closely with business change owners to ensure not only a softer landing of IT changes, but that associated business change is delivered and training contextualised.

c. Within IT we will develop a structured approach to horizon scanning so that we can identify new products and forthcoming features for existing products that may be of significant benefit to the business.

SUPPLIER RESPONSE TO REQUIREMENTS (CONCISE)

1. Supplier Response to Requirements

This section refers to section 3 of your RFT. In our response we replicated your 5 main categories to effectively detail how The Supplier understand and can meet your requirements, as well as demonstrate our experience with regards to the support of the The Customer Infrastructure.

1) Overview
2) Infrastructure Management
3) Service Management
4) Managed Infrastructure Service
5) Continuous Improvement
6) Managing Development Change

1.1 OVERVIEW

Throughout this response we have demonstrated, with detailed responses, sample reports, attached procedures and copies of our processes, the following:

- ITIL-aligned helpdesk
- Networking and security
- Back up
- AD and exchange management
- Availability and capacity management
- Problem management
- Infrastructure updates
- Monitoring services
- Software licensing
- Service desk provision (including portal and metrics)
- Major incident management
- Service delivery management
- Managed builds for software and hardware
- Security and connectivity
- Managed switches, routers and firewalls
- Enterprise management tools
- Cloud management
- Telephony Integration
- Housekeeping
- Resilience, continuity and disaster recovery

We have explained throughout this response how The Supplier can provide the Legal Ombudsman an ITIL Service Management solution which includes the skills, capacity and knowledge to provide both support and enhancement to and on behalf of The Customer.

The Supplier notes the infrastructure inventory, detailed incident volumes, and also the technical descriptions provided as part of the clarifications. In the following sections we outline our approach, expertise and experience in dealing with similar systems and infrastructure environments across our customer base, and how we will address the specific needs of The Customer.

1.2 WAYS OF WORKING

We will ensure The Customer has full visibility of our agreed processes (including progress against KPI's) and that the service provision is transparent and collaborative throughout.

We also ensure our security management approach aligns to our ISO 27001 accreditation meaning The Customer can rest assured it is working with a proven, certified partner that will protect it's assets, systems, people and data during the lifetime of the contract.

- Eliminate the risks associated with significant change such as this
- Ensure that the business and technical knowledge within your current support provider is acquired in as short a time as possible
- Do so in a way that minimises the overhead on your staff and your current supplier.

We will align to the proposed IT governance structure outlined by The Customer. We are familiar operating within a very similar framework for the existing CMS Managed Service we provide to The Customer. Therefore, extending this to the needs and requirements of this infrastructure contract, and proposing many of the same key personnel from The Supplier, will be seamless and provide appropriate governance throughout.

To support this governance model, The Supplier is happy to attend the The Customer offices as required to provide the support required under the contract, but also to align to the The Customer governance structure and ensure effective working relationships between all stakeholders on both sides. We have offices based in Lichfield, and in Studley, providing a local base for our team to operate from when required.

The Supplier will operate a transparent and collaborative service to The Customer, incorporating monthly and quarterly service/ supplier meetings as standard, but also building a genuine partnership (as we have done through our existing CMS contract) which is based on strong relationships at all levels and clear understanding of roles and responsibilities at all times. Regular communication has been key to this over the past 10 months, and we expect to continue and improve this communication whilst broadening the teams and individuals we will have working with The Customer on a daily basis.

1.3 INFRASTRUCTURE MANAGEMENT

All service requests, incidents, problems and changes in the proposed Azure environment will be managed in accordance with our ISO20000 and ISO27001 accredited service management processes.

1.3.1 Networking and Security

The Supplier's Infrastructure Managed Service will be built around delivering and supporting a secure environment for The Customer data, employees, and customers.

We will utilise the skills of our dedicated network engineering practice responsible for design, implementation, and support of local area and wide area network solutions. Comprised of certified architects and engineers, the team has implemented high availability network solutions for a broad number of customers across a range of industry sectors.

The Supplier will deploy enterprise class network products in a high availability network design to eliminate single points of failure. This will ensure network connectivity is always available even in the event of a network component failure.

The Supplier will support the current MPLS solution. We will ensure a fully secured connection by installing a firewall in the L3 Network path. The Supplier support MPLS connections for a number of other clients including Goodbody, 123 and PEAC.

The Supplier provide managed service of firewall devices as part of our Infrastructure Managed Service. These services include

We propose to connect to the The Customer network over a secure site- to-site VPN solution using certificate based authentication.

A dedicated jump server will be implemented behind The Supplier's perimeter firewall (Cisco ASA), and all traffic between the 2 networks will be via a dedicated VPN terminating on The Customer's perimeter firewall. In regard to network design, The Supplier will generally deploy a tiered network architecture whereby traffic can only transit between different network segments via a bespoke set of firewall access rules.

For increased security The Supplier recommends implementing a physically separate perimeter and internal firewalls to ensure complete network segregation.

The Supplier recommends deployment of IDS/IPS on perimeter firewalls to detect and log unauthorised intrusion attempts. Enterprise firewall products The Supplier has implemented and supports include Cisco, Juniper, and Fortinet.

The Supplier will fully support the secure remote access solution deployed in the The Customer environment. We support a wide range of remote client access solutions across our managed service customer base. We understand that each of our customer's organisation maintain their own standards in terms of security and 3rd party access and auditability.

The Supplier recommends multi-factor authentication for all third party client remote access to The Customer's network.

The Supplier has deployed remote access multi-factor authentication solutions using a broad range of authentication factors, including token, certificate, and mobile device authentication. Remote access to The Supplier's corporate network is via 2-factor authentication only, using Microsoft Azure

Authenticator. Additional layers of content control can be achieved through the use of remote device management solutions such as Microsoft Intune.

We will respond fully and promptly to all security audit requests, cooperating and assisting with any security audits and tests as commissioned by The Customer. The Supplier fully recognises the requirement for independent security testing of infrastructure and services, and has participated in this process with a number of its enterprise managed service customers.

The Supplier currently work with 3rd party vendors to assist in scheduled security reviews and Penetration tests.

The Supplier will create a remediation plan and complete the required steps to mitigate any risks identified.

The Supplier successfully achieved ISO27001 accreditation in July 2015. This internationally recognised Information Security standard proves that The Supplier has demonstrated the required levels of control to protect the valuable assets and rights of individuals and clients, and of compliance to all applicable legislation.

The Supplier operates an Integrated Management System (IMS) which integrates all Information Security & IT Service Management processes & policies into one complete framework. The IMS is regularly audited both internally and externally which encompasses our ISO 27001:2013 & ISO 20000:2011 certifications. Our last external IMS audit took place in July 2016 and the next external audit is scheduled to take place in January 2017.

Microsoft, who own the Azure datacentre, is also accredited and fully certified against ISO27001. This internationally recognised information Security standard certifies that we (The Supplier & Microsoft) has demonstrated the required levels of control to protect the valuable assets and rights of individuals and clients, and of compliance to all applicable legislation.

The Supplier can confirm that Microsoft Azure meets the standards required for handling data classified as OFFICIAL under the HMG classification scheme. This means that Microsoft Azure, both the Infrastructure-as-a-Service and Platform-as-a-Service cloud computing platform, are accredited to hold or transact public sector data for business conducted at the OFFICIAL and OFFICIAL - SENSITIVE level of Security Classification. The OFFICIAL accreditation provides additional peace of mind for The Customer. It will deliver confidence that information will continue to stay within the parameters defined by CESG.

For the The Customer hosted solution, The Supplier is proposing Infrastructure-as-a-Service (IaaS), therefore you can be fully confident that the service is accredited to securely host and process all of the The Customer information. Also, as the organisation moves forward and continues to evolve its IT estate you can be confident that future options such as Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) are fully accredited to OFFICIAL.

Microsoft Office 365 is also accredited to OFFICIAL level meaning as The Customer deploys O365, and also considers options for SharePoint Online, you can rest assured that you have a future roadmap which is compliant with the UK Government classification schemes.

Many of our staff are SC cleared and, being an ISO 27001 certified organisation, our internal procedures are set-up to protect and govern the security of our customer's information and data assets.

This certification underpins all of The Supplier's Managed Services policies, procedures and responsibilities, ensuring consistently high levels of service provision to our customers and an absolute focus on information and data security at all times.

In addition to the above, The Supplier will adhere to industry best practice in regard to security hardening of the The Customer network and server infrastructure solutions deployed.

As part of our Infrastructure Managed Service we provide regular server patching to ensure servers are kept up to date with the latest vendor security updates. We will also monitor and are alerted to any new high priority vulnerabilities as they are identified and mitigated against accordingly ensuring client data is protected. The Supplier will ensure that the infrastructure we support is secure and compliant with any regulatory requirements that our customers must adhere to.

The Supplier's own IT security control framework is subject to third party audit and The Supplier is very familiar with the process and rigour applied to the ISO 27001 information security standard.

1.3.2 Backup

The Customer backup process will go through the Supplier transition with an assigned Supplier transition manager. All transitions adhere to ISO 20000 best practice for service transition and as part of this each system will be documented in the The Customer Service Catalogue. The Service Catalogue will detail the following aspects of backup, archive and restore testing for The Customer:

- Schedule
- Retention
- Monitoring
- Error Handling
- Restore schedule
- Failover tests (Business Continuity).

As part of transition, The Supplier will document the end to end existing process for the Backup & Restore service.

This will provide us with the intimate detail we need to support the The Customer backup and restore process. This audit will allow The Supplier to fully understand how your existing backups work (Incremental, Differential, and Full) and provide detail on your backup rotation cycle and data retention policies.

We will work with you to provide advice, planning and support for all media management including implementation of retention policies. The management of the backups will include:

- Maintaining the existing backup schedule and solution.
- Assuming full responsible for media management in your existing data centre. This includes tape mounts, tape rotation and secure off site media management if required.

As part of the transition The Supplier will also strive to reduce backup times, reduce required backup disk/ tape capacity, improve RPO, improve RTO and introduce new backup technologies where appropriate e.g. Azure backup.

All of these improvements will be focused on improving the as-is backup schedules and recovery times. The shorter the RTOs and RPOs, the less downtime the organisation will have to endure, resulting in less productivity loss, less costs incurred and reduced risk of reputational impact.

The Supplier will apply the below 3 methods in order to reduce the RTO and RPO:

- Increase backup Frequency

  An immediate gain to reduce your RTOs and RPOs is to increase the frequency of backups. By doing this, The Supplier will lower the RPO for The Customer due to the availability of more snapshots.

  In parallel, the RTO will be lowered because having more recent backups for The Customer will reduce the time it takes to recover.

- Use of changed block recovery solution

  The concept of changed block technology is similar to incremental backups. Only the blocks of data that have changed since the last full back up or, in the case of virtual machines (VMs), those blocks needed to restore the VM to a given point in time are backed up.

  Whether for virtual or physical backups, if you use a solution that constantly monitors for changes in data blocks then as soon as the backup kicks in, all the pre-processing has already been done. The Supplier will look to implement this approach for The Customer to ensure the overall backup time is reduced.

- Replication

  The Supplier will look to incorporate a live data set that you can switch to instantly in the event of a failure. This approach to backups will help lower the RTOs for The Customer.

The Supplier will support the current as-is backup solution with a view to move to Azure backups over time. We have experience managing Enterprise backup products such as Commvault, ArcServe, VEEAM, HP Data Protector, Netbackup and Microsoft DPM.

Azure backup will allow The Supplier to easily back up (or protect) and restore The Customer data in the Microsoft cloud. Below is an example of the backup policies applied across 3 environments in Azure for one our customers. The Supplier will apply a similar approach for The Customer.

Below is a simple diagram on how Azure backup will work with the Recovery Services Vault:

[REDACTED]

Backups for The Customer will be monitored on a daily basis and checks will be in place via automated reporting to ensure backups have completed successfully. Below is an example of an automated backup report for one of our clients. Backup governance for The Customer will be a combination of manual and automated monitoring via daily reports and OpsView. In the event that a backup has not completed successfully, an incident will be raised and investigated by the Supplier Service Desk. The Customer will be informed of the failure via a logged support ticket. If multiple backup failures occur for The Customer the priority of the ticket logged will be escalated and investigated by the 3rd level Infrastructure team.

[REDACTED]

Any data restore requests that are generated by The Customer will be logged in our call logging tool and carried to completion while in communication with the end user.

The Supplier will provide The Customer with periodic Disaster Recovery testing to ensure the documented Disaster Recovery processes that are in place are accurate and functional. This ensures that in the event of any system failure, the processes and procedures for recovery have been tested and our team are familiar and confident to carry out the steps for The Customer.

Our Disaster Recovery testing will operate on a continued service improvement cycle for The Customer which ensures each test will iron out minor issues identified in the previous tests. Any documentation updates that are required are also carried out at that point. All test restorations for The Customer will be recorded in a backup test log which be accessible on the collaboration site, and a summary report included in the monthly service report. The The Customer monthly service report will have a detailed section on backups highlighting RAG (Red/Amber/Green) status.

The Supplier will manage the backup of The Customer data on a daily basis to include managing secure offsite storage of backup media if required. This will involve reviewing tape backups and removing tapes for offsite transportation. The Supplier manage tape rotation for a number of customers, for example, the Institute of Bankers and UCD.

Outside of the scheduled tasks, The Supplier will also look after ad-hoc backup and restore requests. If a request comes through LANDesk relating to a backup or restore it will be logged as a Service Request and will follow the normal ticket lifecycle to resolution. All test restorations for The Customer will be recorded in a backup test log. An *Example Backup Report* is included as *Appendix J.*

1.3.3 AD and Exchange

Active Directory

The Supplier has extensive experience managing Active Directory environments, including building, maintaining and upgrading. We support customers across wide variety of different AD topologies and levels, and we can confirm we will carry out the below Active Directory tasks for The Customer:

- Group policy reviews and administration
- AD topology and replication administration review (sites and services)
- User and group administration and auditing
- User permissions and password resets
- OU Creation and delegation
- DNS Management
- DHCP Management

For The Customer, The Supplier will monitor and maintain all elements of Active Directory such as group policy updates, event monitoring and support.

Exchange

The Supplier supports customers with varying Exchange versions and infrastructure. We support all versions of Exchange for our customers including on premise, cloud based or hybrid solutions.

For The Customer, we will support the as is exchange environment with a view to migrating to Office365. We have experience in migrating on premise exchange infrastructures to cloud based solutions. Examples of clients where this type of migration was completed are PEAC, Firmus, and Currency Fair. The Supplier has delivered projects for our customers in relation to cross forest exchange migrations, exchange upgrades, exchange decommissioning and migrations from on premise to cloud based platforms.

The Supplier build and deploy exchange environments for our customers, managing them end to end. We have developed checks for application replication technology for Oracle Database, SQL Database and Exchange Server replication. These checks are made periodically and if the expected status is not returned an alert will be raised in OpsView and an incident created for investigation by the Service Desk.

Below is an example of the type of tasks we will manage for The Customer:

- Mailbox moves, creations and modifications
- Email distribution list creation and modification
- Exchange mailbox policies, quota creation and modification
- Modification and creation of transport rules
- Exchange log management
- Modification and creation of exchange connectors
- Exchange patching
- Exchange DNS records (SPF, MX) and domain administration
- Exchange failover tests and cluster checks
- Proactively monitor mail flow
- Exchange audit investigations
- Exchange roles consolidation and installation
- Exchange backups, restores and disaster recovery
- Best practice business continuity for exchange

The Supplier supports a variety of email archiving solutions whether it be archiving in the cloud or onsite. We support customers that use Google Postini archiving, MailMeter and Exchange Online Archiving. Data preservation and integrity are critical for our customers and archiving is integral to a healthy exchange environment.

The Supplier will support Webroot for The Customer. Webroot is a SAAS, cloud based archiving solution that we have supported for other clients

When the transition is made to Office 365, The Supplier will look to utilise the archiving functionality within Office 365 which will allow us to set up archive mailboxes with associated policies for archiving. We can use in-place hold or litigation hold to achieve this goal. Litigation hold allows you to hold all items in the mailbox for a set or indefinite period of time – the items are then easily retrievable should there be a requirement.

As part of the Office 365 offering you can use Litigation Hold and In-Place Hold to accomplish the following goals:

- Place user mailboxes on hold and preserve mailbox items immutably
- Preserve items indefinitely or for a specific duration
- Preserve mailbox items deleted by users or automatic processes such as MRM
- Preserve messages that are forwarded to another mailbox
- Use query-based In-Place Hold to search for and retain items matching specified criteria (you can also place all items hold by including all mailbox content when you create the hold)
- Place a user on multiple holds for different cases or investigations
- Keep holds transparent from the user by not having to suspend MRM
- Use In-Place eDiscovery to search for items that are preserved by being placed on hold.

The Supplier will work with The Customer to identify the most suitable configuration within Office 365 for archiving.

1.3.4 Availability and Capacity Management

Availability Management

Our Availability Management process will be followed to ensure that the Managed Service responsibilities outlined by The Customer are met. The Availability Management process is intended to ensure that all levels of availability match or exceed current and future availability needs of the business in a cost effective manner.

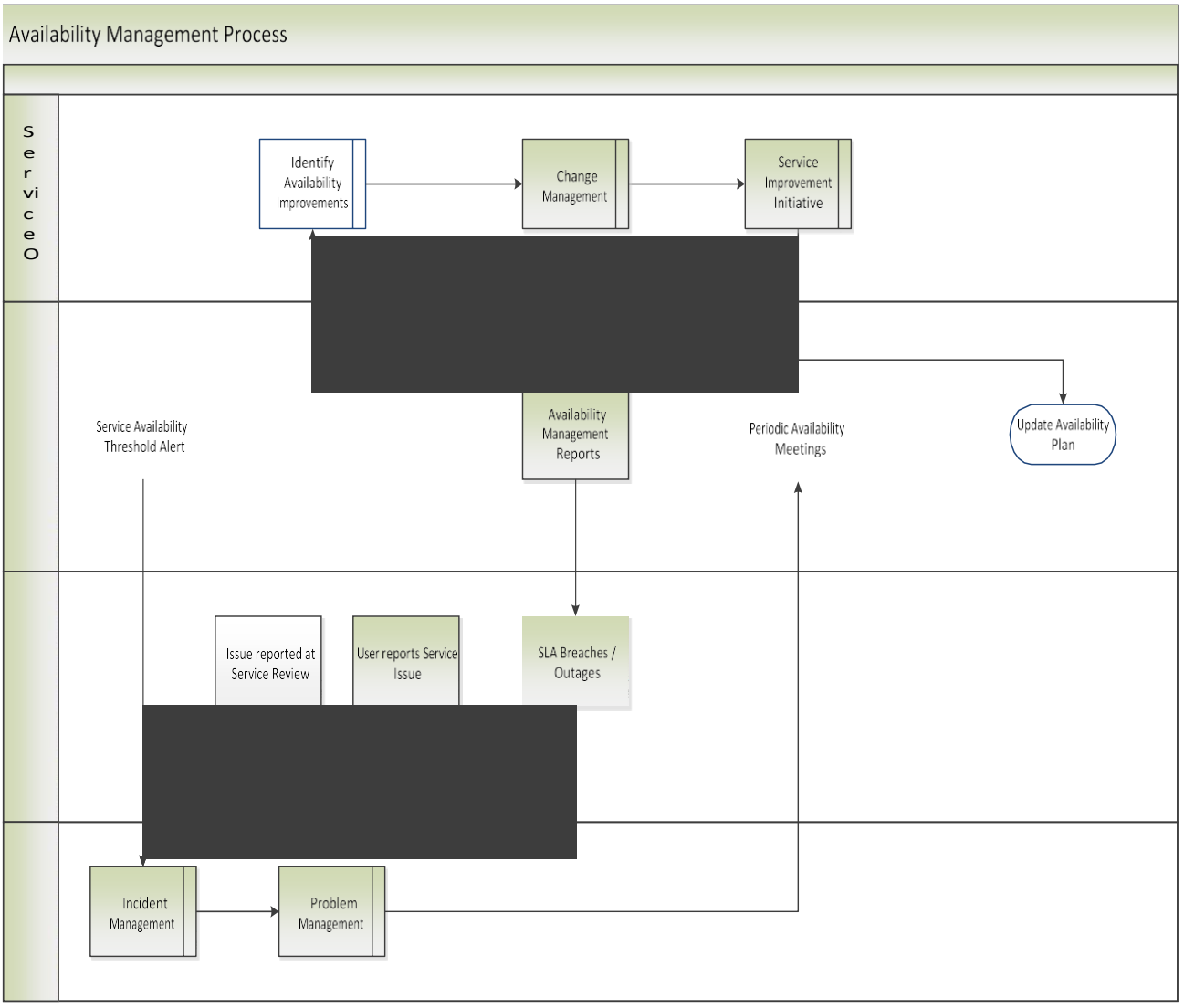
The goal of the Availability Management process is to provide a point of focus and management for all availability related issues, relating to both technology and resources, ensuring that availability targets in all areas are measured and achieved.

As part of the Availability Management process for The Customer, The Supplier will produce an up-to-date Availability plan which will include the identification and design of high availability solutions for critical applications and infrastructure and baseline availability targets across the estate.

Our key objectives for the Availability Management process are to:

- Produce and maintain an up to date Availability Plan
- Provide advice and guidance to The Customer all areas on availability-related issues
- Ensure that service availability achievements meet or exceed all of the agreed Service Level targets
- Assist in the diagnosis and resolution of The Customer availability related Incidents and Problems
- Assess the impact of all changes on the Availability Plan
- Ensure that proactive measures to improve the availability of services are implemented wherever it is cost justifiable to do so
- Ensure availability match or exceed current and future The Customer availability needs.

The Availability Management Process is illustrated below.



[REDACTED]

Key Performance Indicators, (KPIs), will also be measured and reported on. These availability KPIs include the following:

- % Service Available
- % Service Unavailable
- Duration of downtime in service
- Frequency of failure
- Impact of failure
- On end user
- On business transaction process/operations

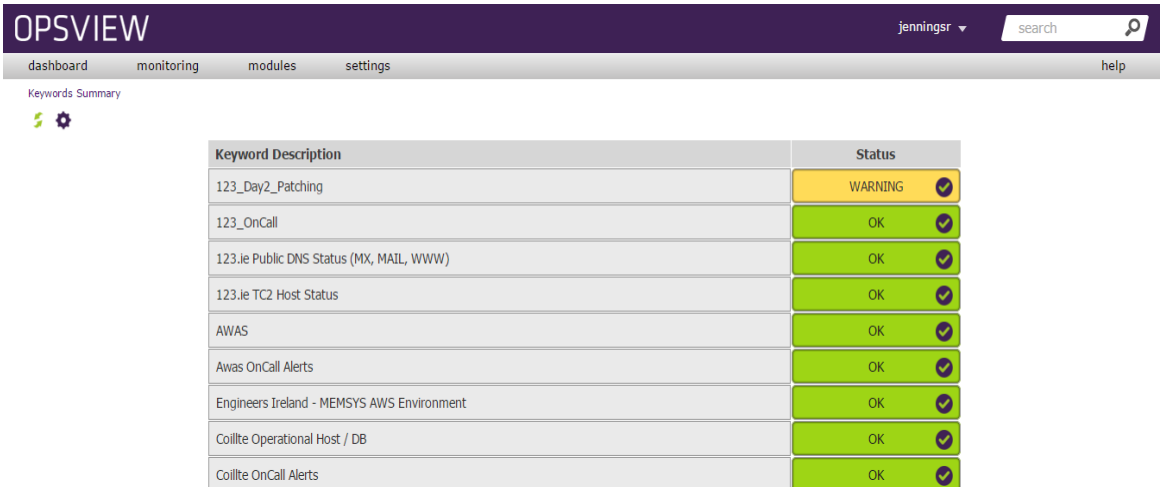
The Customer infrastructure estate will be monitored using the industry leading New Relic monitoring tool. The Supplier will utilise Opsview to provide The Customer with transparent reporting on capacity and availability of IT services. OpsView facilitates the near real time, drill-down component level reporting standards required by The Customer for effective availability and capacity management. Opsview is an extensible tool with a broad range of standard and complex checks, at all levels of the IT estate stack.

We will implement a range of system monitoring covering the key aspects of your environment and systems. Some examples are: capacity of the server disk space, server downtime/uptime, CPU, RAM usage etc.

We will baseline elements of your environment and create thresholds for all aspects of the service. All in-scope infrastructure components will have monitoring agents installed and report back to an Opsview slave.

The monitoring agents will be installed with default values that will cater for automated alerting. The alerting on a per device basis can also be tweaked and refined to better serve the business needs. Breaches of thresholds will trigger an alert. Typically alerts will be set up for warning and critical thresholds. The alert will be visible on the individual screens of our operations control team. In addition, the monitoring solution is visible on a large display hosted in our operations control area.

The figure below shows the summary screen of Opsview used in the Supplier Service Desk. It gives the Service Desk at a glance status of all customer service status in real time.



Opsview also shows the deep level of detail when required. The figure below shows a more detailed view of a Business Service Management (BSM) dashboard for our Service Management System (LANDesk). All the information available and used by The Supplier is by default also available to The Customer in real time simultaneous transmission.

[REDACTED]

Opsview delivers technical information to the Service Management System (LANDesk). This functionality is delivered by the Opsview Data Warehouse (ODW). The ODW, is the long term storage for monitoring data. It converts the data from the Opsview runtime database into an OLAP data warehouse format.

A core requirement for a data warehouse is to not normalise the data too much, yet still allow queries to be easily created. The Supplier can then use SQL to query the ODW and deliver Service based data to the Service Management system. Data from the ODW can be used to build historical SLA reports for customers.

Standard Opsview Reports include:

- Hourly/Daily/Weekly/Monthly Availability Report
- Hourly/Daily/Weekly/Monthly Service Level Report
- Hourly/Daily/Weekly/Monthly Performance Report
- Daily/Weekly/Monthly Event Report
- Daily/Weekly/Monthly Capacity Report
- Daily/Weekly/Monthly Downtime Cost Report
- Weekly/Monthly/Yearly Trend by Service Report
- Weekly/Monthly/Yearly Top Downtime by Service

Filters can be applied to all of these reports to make them specific to customer and service.

See sample Availability report below.

[REDACTED]

The Supplier will use reports like this to collect Service Level data for Service Deliver Managers to deliver SLA reports to The Customer. These will provide one element for discussion in service review meetings.

The Supplier will also be providing The Customer with a Business Service Management dashboard that allows us to deliver a view of both operational data from Opsview and Service Management data from LANDesk. This will allow The Customer to view business services from the near real-time monitoring perspective while also viewing the same managed items from of a business service perspective, thus allowing The Customer to evaluate provision and quality of service.

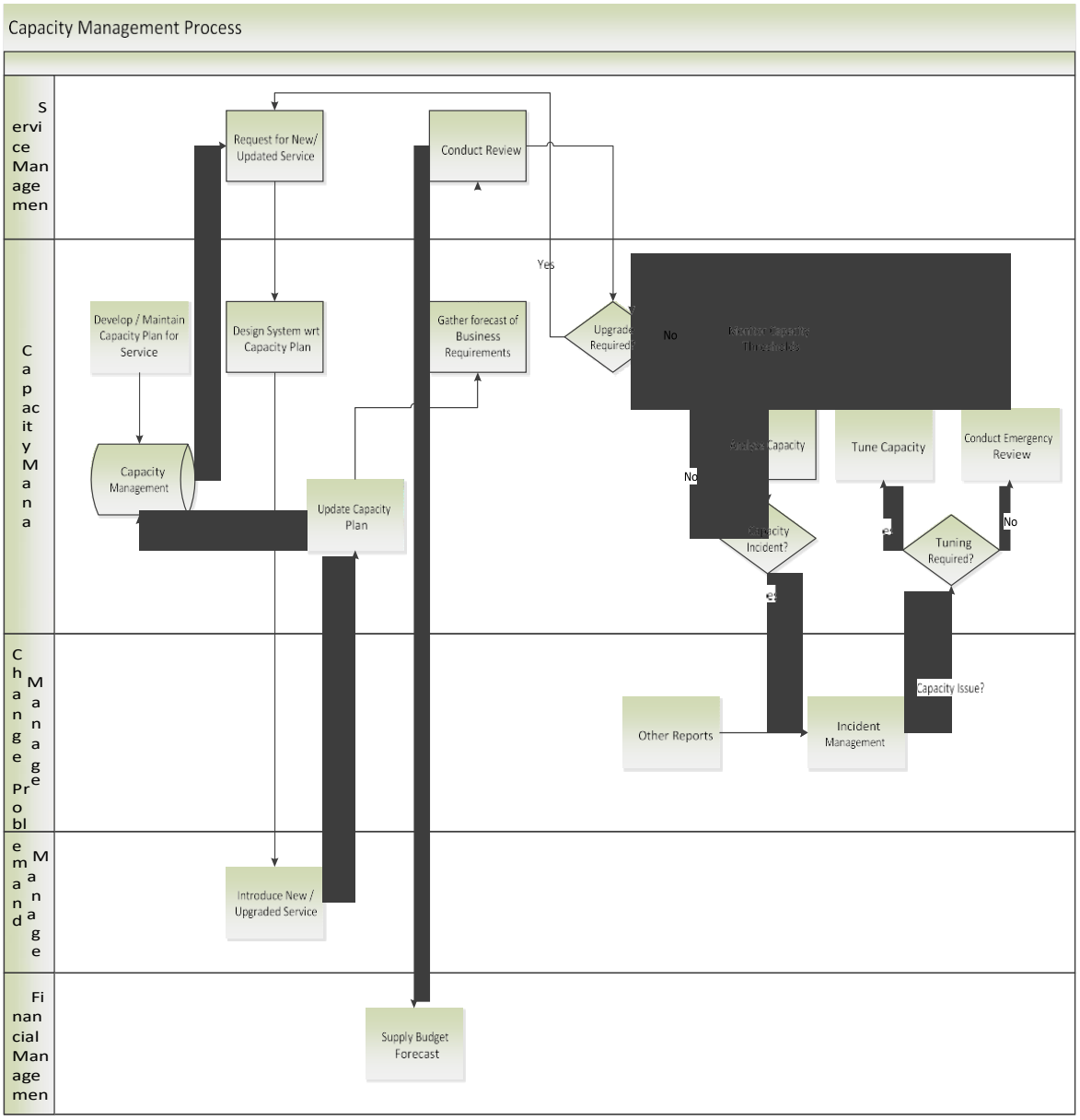
Below is an example of the view from the Business Service Management Dashboard.

[REDACTED]

Capacity Management

The Supplier Capacity Management process will be followed to ensure that the Managed Services responsibilities outlined by The Customer are addressed.

The Capacity Management process ensures that all current and future capacity and performance-related aspects of the The Customer IT infrastructure are provided to meet business requirements at acceptable cost and in a timely manner. The following is our high-level Capacity Management flowchart:



During Transition we will agree your expectations with regard to Capacity Management and the overall process relating to capacity. Thereafter, this process will be the focal point for all The Customer IT performance and capacity issues. Other technical domains, such as Network Support, will carry out the bulk of the relevant day-to-day duties but overall responsibility lies with the Capacity Management process. The process encompasses the production (live) environment for mission critical activities at a minimum, and will include the following components:

- Hardware – from PCs through file, database application servers
- Networking equipment (LAN, WAN, bridges, routers etc.)
- Peripherals (bulk storage devices, printers etc.)
- Software – operating system and network software, in-house developments and purchased packages

- Human Resources, but only where a lack of human resources could result in a capacity-related service impact (e.g. overnight data backups not completed in time because no operators were present to load tapes)

- The primary driver for the Supplier Capacity Management process will be to meet the business requirements of The Customer.
  The Capacity Management process needs to understand the long-term strategy of the The Customer business units while providing information on the latest ideas, trends and technologies being developed by the suppliers of computing and telecoms hardware and software.

In order to ensure clarity with respect to roles and responsibilities we will create a RACI Matrix – the following is a representation of this.

Step	Activity	Capacity Manager	Technical Teams	Change Manager	Financial Manager	Service Management	Incident Management
1	Develop/Maintain Capacity Plan for Service	C	R		C		
2	Request for New/Updated Service	I				R	
3	Design System with Capacity Plan	C	R				
4	Introduce New/Upgraded Service	CI	CI	R		CI	
5	Update Capacity Plan	C	R				
6	Gather Forecast of Business Requirements	I	C		R	C	
7	Conduct Quarterly Review	R	C			C	
8	Supply Budget Forecast	I			R		
9	Upgrade Required?	R	C			C	
10	Monitor Capacity / Performance Thresholds	C	R				
11	Analyse Capacity	A	R				C
12	Capacity Incident?	AC	R				I
13	Incident Management	CI	CI				AR
14	Tuning Required	C	R	C		A	I
15	Tune Capacity	I	R	I		A	I
16	Initiate Emergency Review	AR	C			C	

The purpose of the Supplier Capacity Management process therefore is to:

- Perform demand management for The Customer business, service and resource capacity activities
- Perform modelling for The Customer business, service and resource capacity activities
- Provide application sizing for The Customer business, service and resource capacity activities
- Provide capacity plans for The Customer business, service and resource capacity activities
- Perform capacity monitoring, analysis and tuning activities
- Implement capacity-related changes
- Control storage of capacity data for capacity activities
-
- Provide management information about Capacity Management quality and operations.

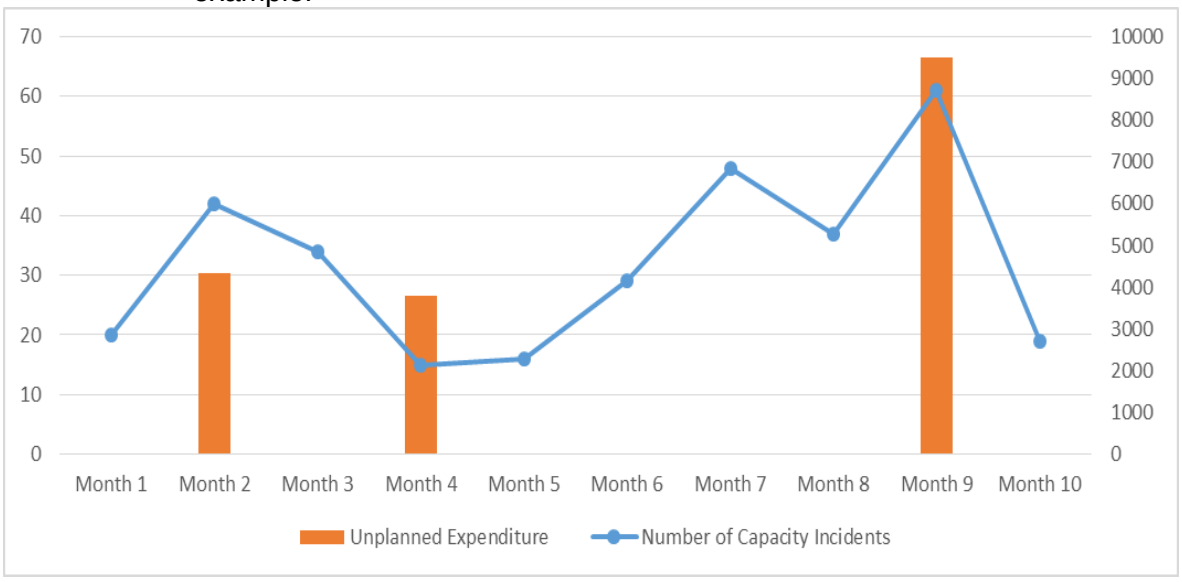
Our key objectives for the Capacity Management process are to:

- To ensure capacity is consistent with existing services and able to match future services (capacity plan)
- Produce and maintain an appropriate and up-to-date Capacity Plan, which reflects the current and future needs of the business
- Provide advice and guidance to all other areas of the business and IT on all capacity- and performance-related issues
- Ensure that service performance meets the agreed Service Level Agreements performance targets, by managing the capacity and performance of both services and resources
- Assist with the diagnosis and resolution of capacity- and performance-related incidents and problems
- Assess the impact of all planned changes on the capacity and performance of all services and resources
- Ensure that proactive measures to improve the performance of services are implemented whenever it is cost-justifiable
- Providing Accurate IT Capacity Forecasts
- Providing Appropriate IT Capacity to Meet Business Needs.

The following Key Performance Indicators (KPIs) will be measured and reported on:

- Percentage reduction in over-capacity of IT, e.g. Storage
- Number of Capacity Related Incidents/Problems
- Percentage reduction in the number of Capacity-related incidents/ problems
- Percentage of changes (marked by Change Management as affecting capacity) assessed for their impact on the capacity and performance
- Percentage of SLA breaches caused by insufficient capacity
- Percentage change in the number of proactive problem resolutions initiated by capacity process
- Percentage accuracy of forecasts of resources utilisation/ workloads
- Cost of spend of unplanned purchases on Capacity.

KPIs will be included in the monthly Service Management pack and will also be published to the Collaboration Site. KPI data will also be graphed. For example:

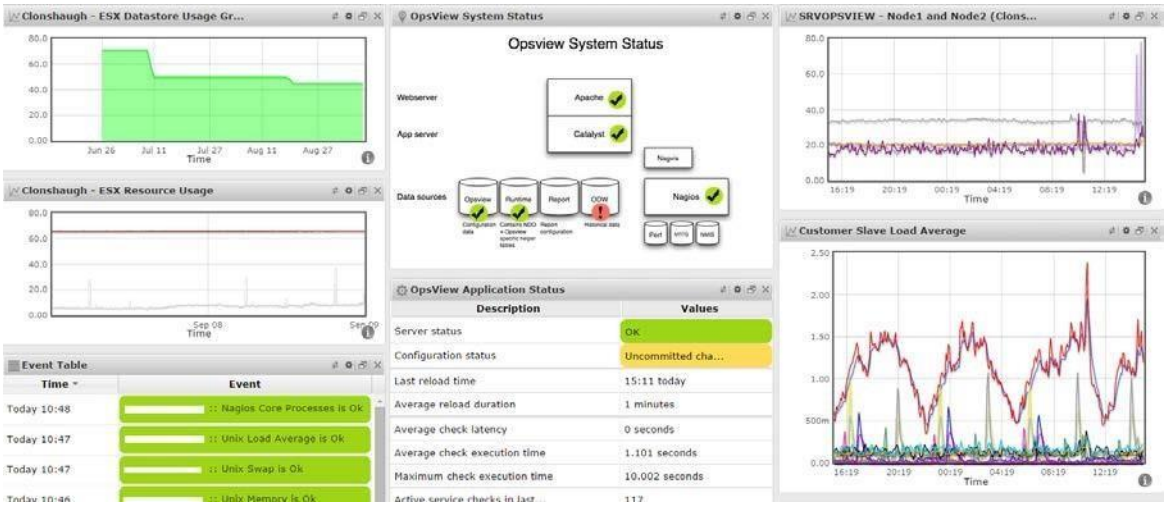


The Supplier will utilise Opsview to provide The Customer with transparent reporting on the capacity of IT services. OpsView facilitates the near real time, drill-down component level reporting standards required by The Customer for effective capacity management. The Opsview Data Warehouse will be used to generate detailed capacity reports for historical trending and analysis with a view to predict future capacity requirements.

Below is an example of a capacity trend analysis report generated for one of our clients.

[REDACTED]

In addition to the above, OpsView also provides inbuilt advanced reporting and analytics of systems events and trends across all services storage, cloud services, servers, virtual machines and applications. These advanced reporting features allow support teams to determine trends and optimise infrastructure planning for future capacity (see below). OpsView is also used to provide Service Level Availability reports to The Customer for your business services, these reports can be scheduled to be emailed to The Customer.



1.3.5 Problem Management

The Supplier has achieved ISO 20000 and ISO 27001 certifications for our Managed Support Services operation across our entire customer support base. The problem management process incorporated by The Supplier is embedded in our ISO 20000 certification ensuring a robust, adaptable and proactive problem management process is provided to our clients.

The primary goals of the Supplier Problem Management process are:

- To prevent incidents from occurring
- To eliminate recurring incidents
- To minimise the impact of incidents that cannot be prevented. In order to achieve this, The Supplier Problem Management seeks to:

- Identify the root cause of incidents
- Document and communicate known errors
- Recommend / initiate actions to improve or correct the situation
- Document and archive knowledge base articles for future use.

The Supplier appreciates that The Customer must meet its commitments to the business and operational organisation and The Supplier has a key role in ensuring that these commitments are honoured.

Our Problem Management policies help to ensure that

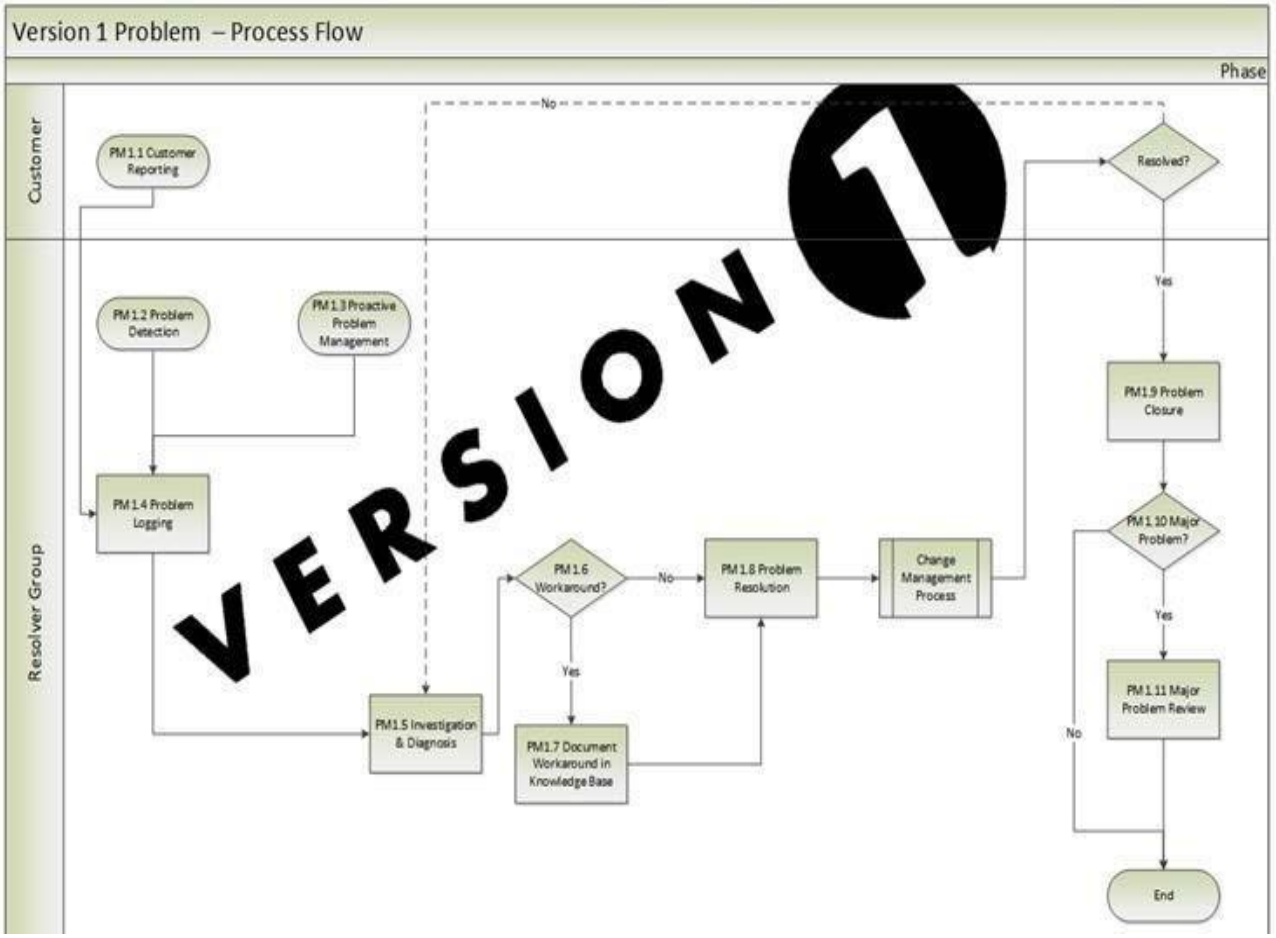
- Problems are tracked separately to incidents. This provides clear separation between incident management activities and problem management activities
- All problems are stored and managed in a single management system. This facilitates reporting and investigation efforts
- Problem records are audited on a regular basis to ensure they are logged and categorised correctly. Audit findings are used to drive continuous service improvements
- Updates on the status of problems are provided in a frequent and timely manner

(as agreed)

- Problems are escalated appropriately in line with agreed parameters linked to Severity and Service Level targets.

The main benefit of this process to The Customer is to minimise the risk and cost associated with underlying problems that are either reported or uncovered during Transition or as part of continual service improvement.

The following swim lane flowchart shows the Supplier Problem Management process. We will modify this if required by agreement with you. It allows The Customer to constantly monitor how problems are being managed and, through analysis, identify if any particular areas of the service or infrastructure are prone to errors.



The Supplier's Problem Management process utilises both Proactive and Reactive problem analysis. Using data from the Incident Management process, proactive analysis is used to identify trends that can point to underlying problems that occur with (for example):

- Specific servers
- Specific applications
- Specific databases
- Specific configuration items
- Specific networks
- Specific users.

Reactive problem analysis is undertaken by the Supplier support team, including the analysis of alerts logged via our monitoring system and incident trend analysis.

In addition, we have a “Possible Problem” mechanism, where consultants can escalate an individual incident for further analysis upon incident resolution.

An example of the application of the problem management process would be for server issues e.g. drive capacity issues, RAM, CPU utilisation, etc. Every time an alert exceeds a warning threshold a ticket is logged via the incident management process and recorded in LANDesk.

Incident management trend analysis is performed on a regular basis to identify repetitive incidents. This trend analysis feeds into the problem management process resulting in the creation of problem tickets.

The root cause of the problem is identified and an appropriate fix for the problem is identified via root cause analysis.

If a change is required a Request for Change (RFC) will be created and brought through the Supplier change management process. All The Supplier changes need to be approved by the Change Advisory Board (CAB) and the customer before being applied. Once the change has been applied a post review of the problem ticket will be performed to ensure the underlying root cause has been resolved. On confirmation of resolution the problem ticket will be resolved. The fix for the issue will be documented in the knowledge base for future reference.

This proactive approach to problem management ensures that The Supplier will reduce down the number of service impacting problems for The Customer. It will also ensure that the knowledge base and associated knowledge base articles are constantly being reviewed and updated.

As stated above, The Supplier maintains a Root Cause Analysis methodology, which culminates in a Root Cause Analysis (RCA) document that is shared with the customer. As part of the Root Cause Analysis we include all identified root causes as well as our recommendation on remediation. The Supplier incorporate the 5 whys methodology into their root cause analysis approach ensuring for a quicker turnaround in terms of resolution time.

We will provide The Customer with a suite of Problem Management reports at a frequency to be agreed as follows:

1. Problem Management Report (Monthly)
2. Service Delivery Report – Problem Management Summary (Monthly)
3. Root Cause Analysis Report - P1 & P2 Incidents.

For example, the monthly Problem Management Report will include:

- The status of all Problems raised during the period (e.g. Draft, Assigned, In Progress, Resolved, Closed, Closed etc.)
- Number and % of New Problems Opened and Closed
- Number and % of Problems Opened and Closed by Priority

- Number of Problems Opened and Closed by Assignee Group
- Trend of status history, e.g. last 3 periods
- Number and status of all Problems since Year start
- Aged Analysis of Open Problems by Team
- Aged Analysis of Open Problems by Priority
- Detail list of all Problems assigned since start of period.

The YTD/Annual Problem Management report will be summarised

1.3.6 Infrastructure Updates

Any proposed changes to the The Customer infrastructure which will affect the systems and services in scope for this Managed Service requirement will be managed under a defined change control process. We have provided our complete Change Control Procedure as part of this submission and this will be found at *Appendix C - V1 - MSP Change Management Process* (included as a separate PDF attached to this submission).

The Supplier Change Management Process is governed by ITIL best Practice and forms a central part of our ISO 20000 certified service.
The objective of the Change Management process is to ensure that changes to all in-scope The Customer Infrastructure IT services and their associated components are recorded and then evaluated, authorised, prioritised, planned, tested, implemented, documented and reviewed in a controlled manner.

Server Patching – Automatic/Manual Updates

The Supplier as part of the The Customer transition will document all aspects of the patching process. A patching schedule will be created which will include maintenance windows for each configuration item (Server)

Server Patching

The following tasks will apply to server patching for The Customer:

- Use of change management process for all patching updates
- Read all related documentation related to the patches being applied
- Apply updates on a needs only basis
- Testing
- Plan to uninstall
- Consistency across Domain Controllers
- Have a working Backup and schedule production downtime
- Always have a back-out plan
- Forewarn helpdesk and key user groups
- The Supplier will ensure that the latest service packs are applied and will never fall more than 2 service packs behind
- Deployment will be done by Phases and target non-critical servers first
- Request for Change will include the patching schedule.

Automatic Updates

Depending on the business requirement and restrictions, server patching can take place on a monthly basis or on a quarterly basis. After an audit of inventory, The Supplier will be able to identify server profiles and create a baseline for the following:

- DEV and UAT or LAB redundant
- DEV and UAT or LAB non redundant
- Production redundant
- Production non redundant.

For redundant servers, The Supplier will automate the process to deploy patches automatically after being approved on the System Center Configuration Manager (SCCM) or Wsus Server (Deployment patch list). To achieve this the Supplier will create maintenance windows containing groups of servers, for example:

- SRVDC01 and SRVDC02 are on the same site and they are domain services redundant
- SRVDC01 - “maintenance window 1” that will automatically update the server every 3rd Tuesday of every month between 01:00 and 03:00
- SRVDC02 - “maintenance window 2” that will automatically update the server every 3rd Tuesday of every month between 03:00 and 05:00
- Both maintenance windows will be updated on the monitoring tool to suspend monitoring during maintenance window hours
- This way if a restart is required during the patching process the service will not be impacted as there is always a DC online supporting the domain services.

As part of the transition The Supplier will be looking for information on the below queries which will feed into the patching schedule and accompanying patching plan:

- For non-redundant servers we will need to know if they are business critical or if they are supporting services or applications that can handle downtime out-of-hours
- If they are supporting a service that can have downtime out-of-hours, a maintenance window should be in place, and all the servers supporting that service or application should be a member of that group.

For example:

- SRVWEB01, SRVDB01, SRVREPORT01 are all supporting APP01

- All servers should be added to “Maintenance Windows APP01” that will Patch and reboot the servers (if necessary) every 3rd Tuesday of each month between 00:00 and 01:00
- As part of the change process downtime should be in place on monitoring and if in production application or service owners should be advised.

Finally, we would end up with a scheduler of automated patching on the servers where automation can happen which will be similar to below:

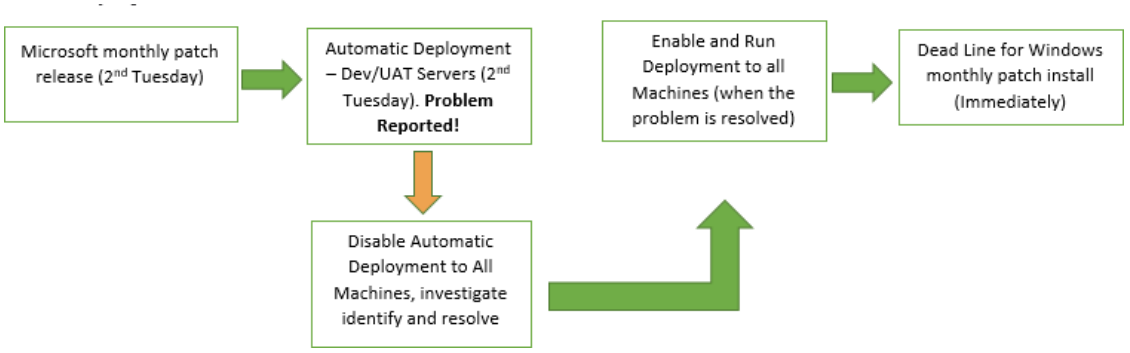
- DEV and UAT or LAB redundant.
  - Maintenance Window 1 – 01:00-03:00 - Every 3rd Tuesday of the month

- Maintenance Window 2 – 03:00-05:00 - Every 3rd Tuesday of the month
- Confirm results
- Request service or application owner approval for production deployment

- DEV and UAT or LAB non redundant.
  - Downtime schedule
  - Maintenance window 1 – 00:00-01:00 - Every 3rd Tuesday of the month
  - Maintenance window 2 – 01:00-02:00 - Every 3rd Tuesday of the month
  - Request service or application owner approval for production deployment

If any issues with patch application arise then a rollback would be performed or a "further investigation and remediation process" will be enacted.

The rollback plane will follow the below process:



A decision will be made to do one of the following:

- Proceed with patching to production
- Removing the faulty patch/patches
- Postpone the Deployment.

Production redundant:

- Maintenance Window 1 – 01:00-03:00 - Every 4rd Tuesday of the month
- Maintenance Window 2 – 03:00-05:00 - Every 4rd Tuesday of the month
- Confirm results

Production non redundant:

- Downtime schedule
- Maintenance window 1 – 00:00-01:00 - Every 4rd Tuesday of the month
- Maintenance window 2 – 01:00-02:00 - Every 4rd Tuesday of the month
- Confirm results

If no Dev or UAT Environment is in place, The Supplier will advise to create a Lab that has some representation of critical services/apps of the production environment so tests can be done on a regular basis.

All server will be monitored by the monitoring tool so if any issues arise after the

Maintenance window end time, alerts will be generated and the incident lifecycle started.

Manual Updates

If Automatic deployments cannot be done, then the traditional manual update should take place. A detailed Runbook will be created with all the manual tasks that need to be done during the Updating process.

This process includes the below tasks

- Approve the patches to the destination machines (via WSUS or SCCM)
- Follow the patching process runbook for the machine
- Verify that monitoring is working as expected post update

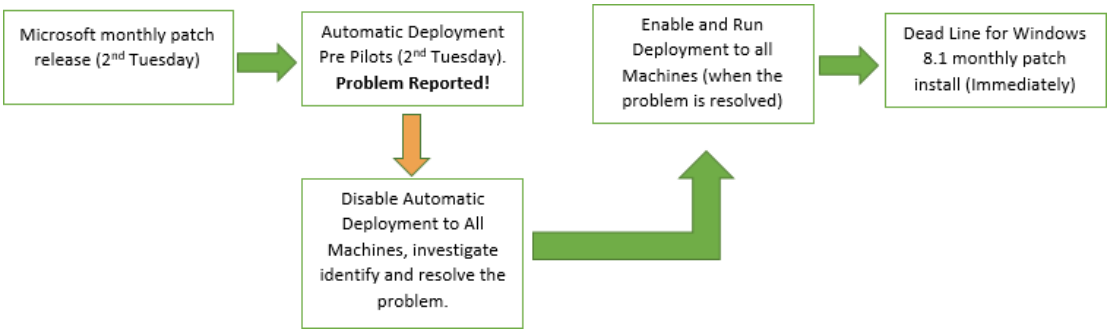
Desktop Patching

The following tasks will apply to desktop patching for The Customer:

- Use of change management process for all patching updates
- Read all related documentation related to the patches being applied
- Apply updates on a needs only basis
- Testing
- Always have a back-out plan
- Don't get more than 2 service packs or OS major releases behind
- With windows 10 and SCCM we can use the Servicing feature and have an integrated solution to manage release versions as they become available
- Deployment will be done by Phases and Target non-critical machines first
- Patches should be applied to 2 test groups before go live to all users
    - 1 smaller group that has good IT knowledge and will get the updates when they are released
    - 1 UAT group that should represent all company areas in order to identify possible issues or incompatibilities if they arise.

Below is an example from one of our clients highlighting 3 collections (UAT 1, UAT 2 and all users) created in SCCM to cater for 3 distinct Desktop software update groups

The below rollback process is followed if any issues with the applied patches are encountered.



If an issue is identified on the Pre-Pilot Machines via UAT it gets reported to The Supplier service desk team. The collection for all users will be disabled manually on the SCCM Server, while the issue is being investigated.

If investigation leads to a faulty patch, the patch will be removed from all deployments. The membership of the software update can be edited to remove any faulty patches

Desktop patching will be applied on a monthly basis for all windows devices and will address:

- Security updates for MS Operating Systems
  - Critical Updates
  - Important updates
- Office Updates.

1.4 SERVICE MANAGEMENT

The Supplier will provide The Customer with an ITIL Service Management solution which includes the skills, capacity and knowledge to provide both support and ongoing enhancement to The Customer across all elements of your ICT landscape deployed on premise and in Azure.

Our commitment to The Customer is that all of the services we provide will be ISO 27001 and 20000 compliant and will fully align to agreed SLA's supporting the service.

We will work with you to ensure our processes operate in line with ITIL and are also aligned with The Customer's regulatory obligations and other business requirements.

In parallel with the environment build, we will carry out Discovery and knowledge transfer which will allow us to assume full responsibility for managed support of the The Customer infrastructure estate when migrated to Azure. This will require joint working with the incumbent provider to support both the Discovery activities, and the controlled transitional activities into the new infrastructure environment.

Once the new The Customer infrastructure environment is provisioned in Azure we will begin to migrate all in scope services to Azure on a phased basis.

Once each service is successfully migrated and tested in Azure we will assume full support from that environment and the legacy environment can then be decommissioned.

We believe this to be the preferred, and lowest risk, approach for The Customer to minimise any disruption to your staff during migration but also to ensure continuity of service. We have taken this approach for many other customers and given the time considerations regarding the incumbent providers current contract, this approach will also be in line with The Customer requirements.

Once all services are fully transitioned, tested to be operational and performing in line with The Customer requirements relating to performance and availability, the legacy environments previously hosted by the current incumbent can be decommissioned and the full service operated from Azure and The Supplier's Managed Service from this point onwards. We expect this full transition and migration project to take a total of 17 weeks.

As mentioned above, it is imperative that The Customer, and The Supplier, has the support and collaboration required from the incumbent provider during the transition and migration phases of the project.

Also, depending on when The Customer award the contract and relevant paperwork is completed, consideration must be given to the expected timescales for transition and migration and how that aligns to the incumbent supplier's contract.

Depending on the date of expiry of that contract, The Customer may need to consider options for extension for a period to cover any time where their service is required beyond that expiry. We have included further detail on the expected dates to support the transition and migration project in *Section 3.4.1*, and would be pleased to discuss this further with The Customer.

Once all The Customer services are live in the new Azure environment and under full Supplier managed support we can guarantee that we will operate the service in line with SLA's agreed with The Customer. This is a dedicated support practice with over 250 staff who are certified across all the technologies and the methodologies we employ, extending to the full technology stack required by The Customer for this infrastructure managed service.

Our manned 24-hour Operations Centre will conduct continuous health checks to verify system performance and availability of the The Customer infrastructure estate.

More importantly, The Supplier will focus on business application and process monitoring, not just technology elements. Automated alert and business event correlation technologies let us investigate and resolve potential issues in real-time, before they impact business continuity. This enables us to identify outages and potential issues before The Customer do (we call you before you call us) and achieve lower Mean Time to Repair (MTTR) through improved data integrity and infrastructure management, and also adhere to agreed SLA's.

In addition to the service transition and migration, and commencement of full managed support from Azure, we have also explained throughout our response to *Section 3.4* how we will effectively operate the support service, integrate with the The Customer operation, govern our service performance and contractual obligations, and also how we will continually work in partnership with your organisation to improve our service to you. We look forward to discussing this in further detail with The Customer should be called to present our solution to you.

SharePoint Online

Based on the information provided regarding The Customer's current intranet, moving the application from the current SharePoint platform to SharePoint Online should be relatively straight forward and something The Supplier has undertaken previously for other customers. The Supplier has extensive experience of moving our clients from SharePoint on premise to SharePoint Online (e.g. Bank of Ireland which had >15,000 users, over 2TB of content and 8,000 site collections). Moving from SharePoint on premise to SharePoint Online is a migration exercise, rather than an upgrade.

Our experience in SharePoint support and development is well proven and we are confident we can deliver against the specific requirements as outlined by The Customer.

Exit Management Plan

Our objective is to extend the existing relationship we have established with the Legal Ombudsman over the past 10 months, and would hope this lasts long into the future, however we do recognise that there are occasions where you may seek to change vendor in future.

Should that arise, The Supplier is committed to working in your best interests with whatever vendor you select.

Because of our team-based approach, we endeavour to reduce the reliance on individual knowledge and expertise in the execution of support services, so all documentation is maintained and updated over time as a matter of course.

In addition, our ISO-certified transition process specifies that a 3-month review of the process must be conducted (and is auditable by our external auditors). Following on from this review, we propose to update the exit plan, with any learning or changes recommended following the initial transition, and will agree this with you.

We also commit to maintaining this plan on a regular basis, and in the event of any significant changes that warrant additional updates or amendments we will notify The Customer.

Our recommendation is that a similar process and associated indicative plan to that described above for transition be utilised, although we expect that an incoming vendor may propose an alternative and we will work with them to ensure its success.

The Exit Management Plan is included as a final step in The Supplier's Service Transition Methodology listed as de-transition services. As each de-transition can vary based on each individual service or project the steps out lined below are used to identify the specific tasks that must be completed by all relevant parties in order to successfully sign-off a transition by the Change Approval Board in accordance with the ISO 20000 accreditation.

De-transition checklist

The project's transition manager creates a de-transition check list for the system on the Transition SharePoint site. This checklist will be used to ensure that all relevant transition tasks are completed as part of the project transition. A Sample transition (Exit) checklist has been shown.

	Project Tasks	
	De-transition IPC logged?	
	Have all internal stakeholders been made aware of the de-transition? (including Team Lead, SDM and Account Manager)	
	Are all IPCs resolved or outstanding items agreed with the customer?	

	Set the project status on the intranet to "complete"	
	Has the project been changed to inactive in LANDesk (can't happen until all activity on project is complete)	
	An internal closeout report will be created by the SDM and distributed to the MSP Practice Head	
	An external closeout report may be created by the SDM and distributed to the MSP Practice Head and the appropriate Team Lead for review and then to the client.	
	FSC Entry complete and approved?	
	On-Call Manuals updated?	
	Where support service is changed it is critically important that documentation is updated.	
	Review of Transition Plan with The Customer's new service provider	
	Document handover to The Customer and The Customer's new service provider	
	System walkthrough with The Customer's new service provider	
	Known issues review with The Customer's new service provider	
	System review with The Customer's new service provider	
	Customer Communication	
	Written/verbal notification of termination of services received from client (if verbal a notice in writing has been requested	
	Customer notified that DDD's must be consumed within notice period or balance will be set to zero	
	Is knowledge transfer between support team/customer/3rd parties complete?	
	Production	
	Documentation/hardware/ handed over to The	

	Customer	
	Security fobs been handed over to Client where relevant?	
	Have appropriate monitoring applications been removed from servers (hoststats/statspack for monthly checks, nagios slave if using Opsview)	
	Have backups and back email alerts been disabled?	
	Have all tasks been removed from the Scheduler	
	Have passwords been removed from PMP and u/ns and p/ws communicated to the client in a secure manner if required?	
	Has the VPN been disconnected?	
	Any customer equipment (Fobs, PCs etc) identi-fied and returned to customer (with signoff)?	
	Commercial	
	If a de-transition charge is required, has it been set up and invoiced?	
	Billing complete?	
	If an archive licence is required has it been set up and invoiced?	

Log a change in the FSC

Once all de-transition activities are complete, the SDM must log a change request within the forward sched-ule of changes and seek approval from the change board.

Due to the de-transition being a sub process of transition & support, time estimates for the completion of a transition are determined by the priority of the de-transition IPC raised which will still adhere to the SLA's for IPCs agreed as part of the support contract. contract.

1.4.1 Monitoring Services

The Supplier provides real time proactive monitoring as a key element of the managed service offering based on OpsView. OpsView is an award winning, open source Nagios based monitoring, alerting and trending tool and is the foundation stone of our offering to customers for the monitoring and transparent reporting of ongoing performance, capacity and availability of IT services. We have been using OpsView since 2009 and Nagios since 2006 and at time of writing The Supplier monitors over 27,000 daily checks over 80 cus-tomer estates across all industry sectors.

OpsView is an extensible tool with a broad range of standard and complex checks, at all

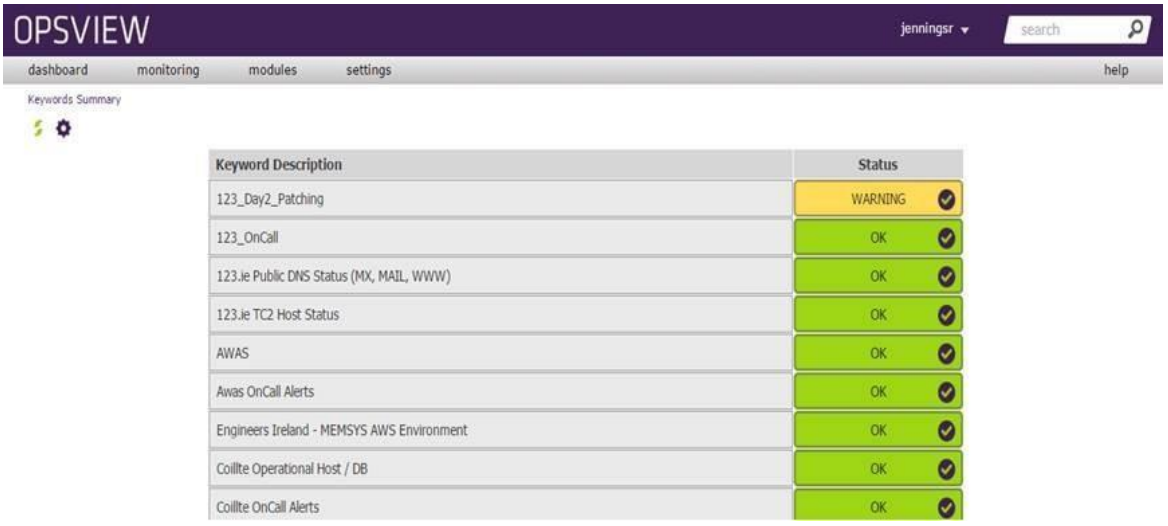
levels of the IT estate stack. It is an IT systems management leader with hundreds of global enterprise customers, including blue-chip organizations such as BT, Blue Cross Blue Shield, BSkyB, Allianz, US Army, IBM, Cisco, MIT and Irish Revenue. OpsView can detect the warning signs of an impending failure so that The Supplier's support staff can resolve the issue before it causes down time and an associated productivity loss.

It brings together all the information our support team require for highly effective operations and support. Over the years The Supplier has developed a library of checks that are available for reuse. For server operating systems parameters such as uptime, CPU utilisation, disk capacity and RAM usage are included in the standard checks. For server hardware parameters such as hard drive failure, redundant power supply failure and temperature issues. For database servers, The Supplier monitors backups and data- pump exports, database availability, tablespace usage and alert logs.

The Supplier will tailor our proactive monitors and alerts for the The Customer environment. The Supplier has developers on-hand who can create custom monitoring checks should the requirement arise. For example, Airtricity have a customer polling suite that polls specific user activities, such as login to the billing platforms, and metrics for databases and applications that The Supplier developed and manage.

Opsview will be integrated into existing The Customer monitoring systems and will be used as a Manager of Managers (MoM). This will give The Supplier staff visibility of the whole The Customer estate as appropriate.

The figure below shows the summary screen of Opsview used in the Supplier Service Desk. It gives the Service Desk at a glance status of all customer service status. This allows the Service Desk to be SLA focussed by reacting to monitoring events as soon as they are triggered.



The open nature of Opsview has allowed The Supplier to develop an event focussed Opsview dashboard for the Service Desk. This is displayed on the Service Desk monitoring screen and allows for event focussed monitoring. Note the item highlighted in yellow indicates that an event is at a soft/hard alert. One bar means that a single poll has failed and there is risk of an actual impacting event and that additional polls have been

triggered. Three bars indicate a hard actionable event. This functionality can be customised to create a hard failure on the first poll failure.

As our primary Monitoring tool, the preferred monitoring is achieved using northbound interfaces or plug-ins from vendor monitoring tools to capture data for OpsView. In some instances, a NBI or Plugin is either not available or viable and email notifications from the monitoring tools are the most practical solution. In this scenario, The Supplier will configure the relevant monitoring station to forward email to the 24x7 Service Desk monitoring mailbox. This mailbox is monitored by the Service Desk who will trigger standard alerting practice based on run books or escalation matrices.

The Supplier's Monitoring solution is managed by our 24x7x365 Service Desk team. Our Service Desk is ISO20000 and ISO27001 accredited and they proactively monitor, detect and very often fix problems before they happen to avoid expensive down time or associated productivity loss. In addition, live monitoring is enhanced by the use of extensive runbooks and escalation matrices which are used to initiate pre-emptive action.

OpsView is designed to provide full visibility of an entire IT estate, providing visibility to each and every layer of the IT infrastructure in a tiered configuration. OpsView facilitates the near real time, drill-down component level reporting which can be grouped together in logical displays that suit the specific priorities and interests of The Customer and is available to both The Supplier consultants and individual customers through a web portal.

For example, The Supplier has developed customer specific storage monitors for Dell, EMC and HP storage environments for customers such as 123.ie, Irish Continental Group and Goodbody Stockbrokers.

The Supplier can provide access to monitoring dashboards for The Customer to ensure the service is fully transparent and you can view exactly how the The Customer infrastructure estate is performing.

An example of some monitors for one of our managed service storage customers is displayed below:

Host	Service	Status	Last Check	#	Status Information
Primary_SAN	Controller Node Status	OK	2016-09-15 20:01:53	1/3	OK : All nodes have normal status
	Fibre Channel Capacity	OK	2016-09-15 20:03:23	1/3	OK : Used FC capacity = 66%
	Fibre Channel Ports	OK	2016-09-15 20:02:08	1/3	OK : All FC ports have normal status (ready or offline)
	Logical Disks	OK	2016-09-15 20:02:43	1/3	OK : All LDs have normal status
	Physical Disks	OK	2016-09-15 20:01:43	1/3	OK : All PDs have normal status
	Power Supply	OK	2016-09-15 20:01:08	1/3	OK : All nodes have normal status OK : All nodes have normal status
	Virtual Volumes	OK	2016-09-15 20:01:38	1/3	OK : All VVs are normal
	Connectivity - LAN	OK	2016-09-15 20:01:18	1/3	OK - 10.25.9.170: rta 0.359ms, lost 0%
Totals	8	8 OK			

The Supplier's storage proactive monitoring will monitor storage metrics such as capacity and availability. These metrics will have thresholds set which when breached will raise an alert which the operations centre will be pick up and an incident be raised and triaged to the appropriate team for investigation. Storage relation incidents will then be triaged to the storage administration team. The Supplier monitor storage devices for other managed service customers such as Goodbody Stockbrokers, Irish Continental Group and PEAC Finance. The Supplier also have partnerships in place with EMC and HP that allow us the ability to work directly with the vendor in the event that there is a major issue.

As mentioned, OpsView facilitates the near real time, drill-down component level reporting which can be grouped together in logical displays that suit the specific priorities and interests of The Customer and is available to both The Supplier consultants and individual customers through a web portal.

This allows customers to login via a web portal and get a full view of active alerts within their infrastructure and to drill-down to the individual component. Opsview allows us to not only capture live data but also to store it to provide visual historical trends of data growth, processor usage, available capacity, etc. These trends cover all layers of the infrastructure such as physical and virtual storage, physical hosts, Windows and Linux virtual machines, databases, application and websites. The various views selected below represent a sample of the views that are available to customers.

Digital Dashboard Views - Server View

Groups can be configured to your needs so we can monitor servers by location, operating system, function or any grouping that you require.

The Supplier currently maintains the capability to report back all levels of component performance and data tracking, cascading from the business application level down to the individual component.

1.4.2 Software Asset Management

The Supplier has a dedicated Software Asset Management and Licence Consultancy practice who handle all of our Software Asset Management processes including procurement, invoicing, inventory, licence optimisations, contract negotiations, management and renewals. We have operated a focussed SAM team for over 15 years, and count many large enterprises across Public and Private sectors amongst our customer base, including Transport for London (TfL), Severn Trent Water, Scottish Water, NHS Wales, Student Loans Company and Plymouth University.

The Customer requires The Supplier support it in ensuring that it remains compliant in regards to licencing and/or subscriptions for all components of the Infrastructure Service. The Customer requires that the MSP supports licensing across the Microsoft EA and those required for services from other third party suppliers.

To deliver this Microsoft specific software asset management service, The Supplier will draw on our experience with similar private sector & government projects in the areas of:

- Software licence position development
- Software audit readiness
- Software Asset Management “SAM” program development
- SAM as a managed service.

Using this experience The Supplier will assist The Customer with optimising its Microsoft software investments through the creation of several key software asset management deliverables including:

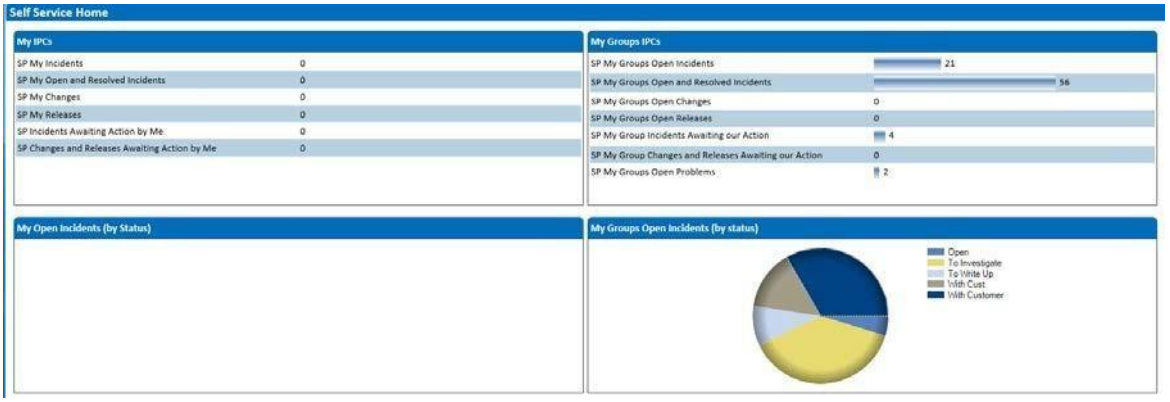
- License Review Findings Report
- Effective License Position
- Microsoft Install & Entitlement Registry
- Independent Microsoft License Advice
- Calculation of Microsoft True Up Requirements.

By delivering services linked to industry best practice the Supplier project team aim to achieve the following project objectives:

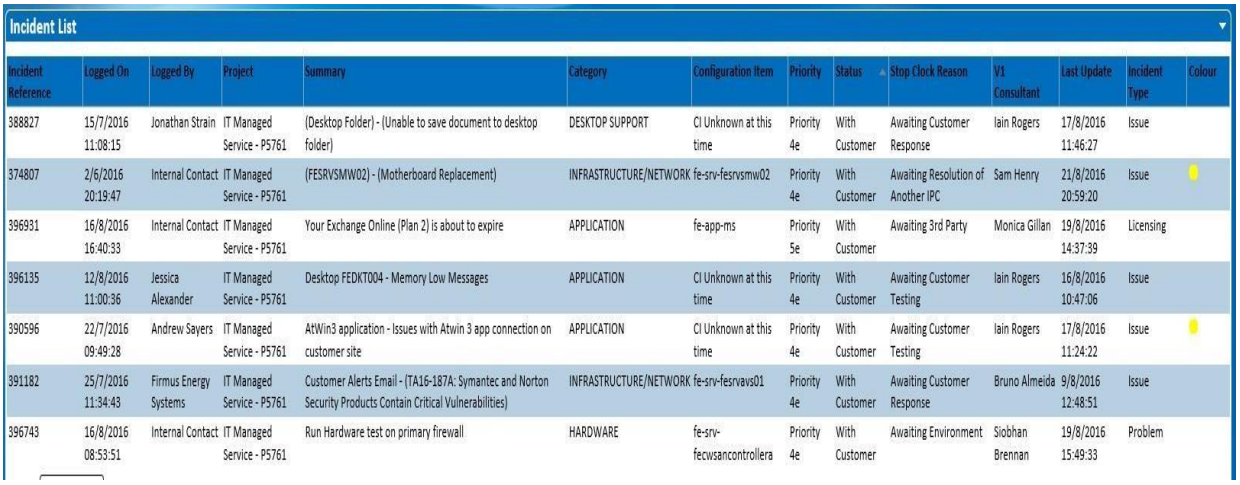
- Compile and analyse proof of Microsoft license entitlement
- Collect install & usage data
- Analyse usage relative to Microsoft product use rights
- Independently verify The Customer effective Microsoft license position including under / over licensing and any breach of Microsoft license use rights
- Document & present findings including possible optimisation
- Lay the foundation for effective ongoing Microsoft license management
- Enable the Customer to proactively manage the potential risk of a Microsoft led audit

- Prevent possible waste and redundancy associated with poorly optimised license entitlement
- Support optimised true ups.

Service Management Dashboard



The Supplier's Service Management Dashboard gives you an online, drill-down view of the quantity and status of all IPC (Incident, Problem, Change) tickets currently open. Clicking on the status or priority of a call gives drill-down views, with update information and colour coded indicators of SLA



Service Management Drilldown

The Supplier will provide a fully supported Service Desk with dedicated lines and staff to respond to incidents, resource requests, requests for change (RFC) or queries raised by

The Customer. The Service Desk will comply with the incident response times agreed between The Customer and The Supplier. We also maintain a “Forward Schedule of Change” which outlines all planned changes and which is reviewed by our Change Advisory Board (CAB) on a weekly basis (further detail on this process is included in *Section 3.7.5*)

This Service Desk will support the following services for The Customer:

- Logging of incident or e-mail request and supplying The Customer with a unique reference number.
- Closing of The Customer logged incidents when required.
- Incident tracking and reporting.
- Passing of incidents to the The Customer support team for response.

The methods of contacting The Supplier Service Desk are as follows:

[REDACTED]

To complement our LANDesk tool, we maintain an internal Customer (SharePoint) site for all our managed services customers. The site has strict governance and is password protected. The site is used as a knowledge repository for the project. Typical information stored in the repository includes:

- Terms of Reference - describing the scope of the service
- Overview - English descriptions of the project and service provided
- Technical information – e.g. source code location, database schema etc.
- Remote connection - Details on how to connect to the customer site
- Monthly and Quarterly reports – archive of previous and current service reports
- Health check reports – archive of previous and current service reports
- System Architecture diagrams - system documentation & architecture diagrams
- Configuration management – identified configuration items and diagrams
- Operational process – project or service related documents, process descriptions
- Knowledge Base – resolution to common issues, run sheets, process descriptions etc.
- System checks – record of manual system checks and frequency to be carried out by our Operations Control team
- Any customer or project related documents.

Information Security Management

As a provider of IT managed services to customers in the public sector, The Supplier fully understands the importance of a robust IT security framework to The Customer.

The development of The Supplier's Information Security Policy is carried out under the "Plan, Do, Check, Act" mechanism described in the Integrated Management System (IMS) Governance Process, which is stored in the Policy & Process library on the Supplier intranet. These standards are in accordance with ITIL guidelines, and ISO20000 and ISO27001 standards.

The Supplier Directors have approved and authorised this Information Security Policy for the company. The policy is authorised for separate distribution under the Chief Executive's signature. A current version of this document is available to all The Supplier employees and to external parties when signing supply contracts.

It is the policy of The Supplier to ensure that:

- Risk to the information assets of the company and its clients are identified and evaluated
- Information is protected against unauthorised access
- Confidentiality, Integrity and Availability of information is maintained
- Regulatory, legislative, business or contractual security obligations are met
- Business Continuity plans will be produced, maintained and tested.

The Supplier has implemented the IMS to manage Information Security and IT Service management to the highest international standards. An Information Security Officer along with the IT Governance Committee are responsible for maintaining the policy, as well as providing advice and guidance in its implementation. Details of the IMS and the associated roles and responsibilities can be provided on request.

The Supplier requires that all breaches of information security, actual or suspected, will be reported to the Service Desk (servicedesk@The Supplier.com). The IT Governance Committee, chaired by the Information Security Officer, reviews and manages all Security Incidents.

The Supplier undertakes to provide appropriate information security training for all employees. It is also the responsibility of all The Supplier employees to read, sign, and adhere to this policy as part of their employment contract, as standard process. We have also developed “Data Protection and Information Security” awareness training that is mandatory for all employees and contractors. This training is conducted on a companywide basis and now runs on a recurring basis once per quarter and is also covered in our Induction process.

All employees, contractors and third party suppliers working for, or providing services to, Version

1 are required to ensure that the confidentiality, integrity, availability, and regulatory requirements of all business systems are met.

This policy is fully reviewed for effectiveness and suitability annually as part of the management review process, as well as by external auditors to retain ISO20000 and ISO27001 accreditation.

1.4.3 Service Desk Function

The Supplier confirms that we will provide a service desk function to The Customer between 07:30 and 19:00 Monday to Friday (excluding bank holidays) and will provide a fully monitored 24*7 service outside of these core business hours, with the ability to handle any P1 incidents raised outside of the core hours.

Our team will be fully resourced to meet the support requirements for The Customer and cover is ensured for all elements of the service within required hours. We can also confirm that should a critical incident occur, for example, at 18.30 and not be resolved by 19:00, then our team will continue to work on the incident until it is resolved to the satisfaction of the The Customer. This is a core requirement for all of our Managed Services customers and a service we deliver to numerous Public Sector bodies across all of our service lines.

All service tickets are received by the Service Desk. The incident is opened by The Customer reporting an issue. The Customer can also log issues via the Supplier customer portal at https://my.The Supplier.com/ and incidents can also be auto generated where automated alerting is in use, as a result of an alert being received.

An email confirming that the incident has been logged is automatically sent to the customer. The email confirms:

- Log Date & Time
- Reference Number
- Information how The Customer can update/chase up/escalate the issue.
- An expected update or resolution time

Set the Priority

There are 5 priority levels, P1 to P5; P1 being the most urgent.

Once an incident is logged with the Service Desk it may be escalated from its default priority to a higher level.

To escalate an issue to a higher priority level, phone the Service Desk with your Service Desk reference number and ask that the issue be escalated and give the reasons for the change. You may also wish to specify the frequency with which you want a progress update.

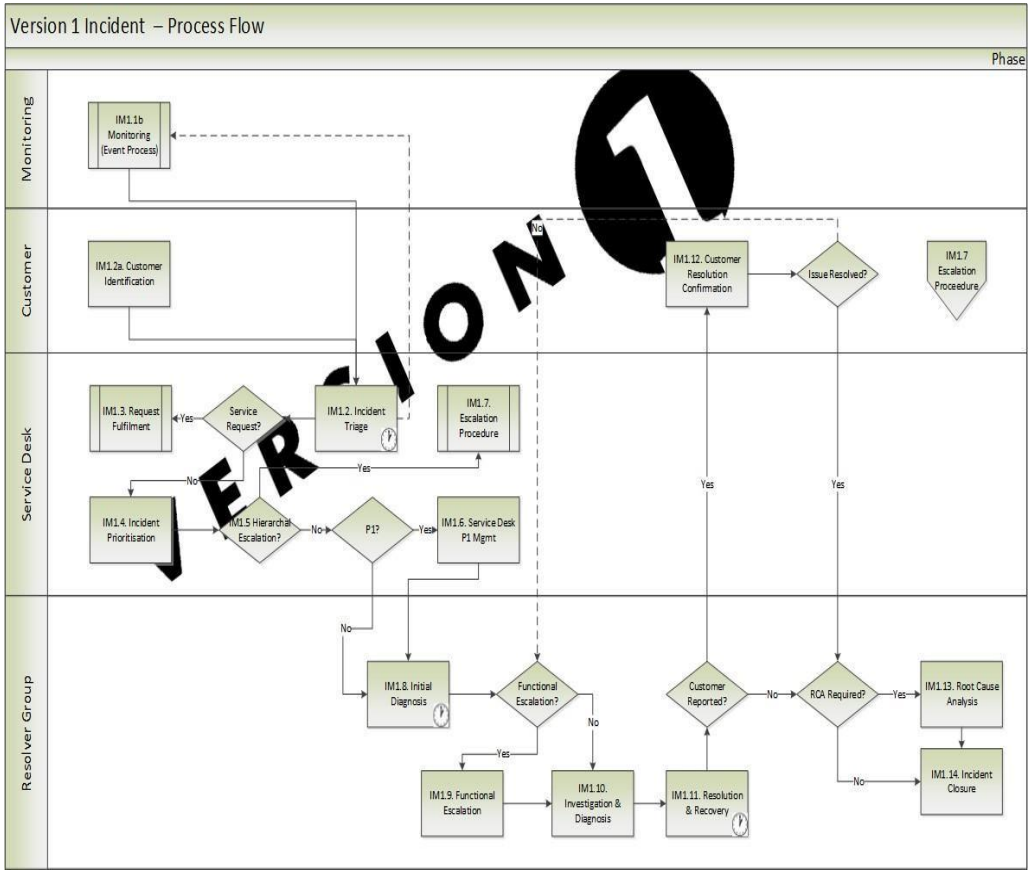
We have included in *Section 3.4.11 – Escalation Routes*, a detailed overview of the Supplier escalation process and how this is handled in the event The Customer needs to escalate any incident or issue.

The table below contains the contact details of those involved in the delivery and support of the service from The Supplier. Each individual will have accountability in the The Customer relationship/contract and will be focused on building stable peer relationships with The Customer to facilitate timely and helpful action in the event of an issue arising in either organisation. These named individuals will be aligned to the escalation route defined by The Customer and will be available as required throughout the contract relationship.

[REDACTED]

[REDACTED]

Incident Management Process



IM1.1 Incident Triage IM1.1 Incident Triage

Incident Triage is the process of identifying, logging and categorising incidents. Each of these steps is explained in detail below.

IM1.2 Incident Identification

Work cannot begin on an incident until it has been verified that the incident has occurred, however it is unacceptable to wait until a user contacts the Service Desk to do this. Therefore, if it is not possible to verify that the incident has occurred within a reasonable timeframe, the incident should be progressed so the issue can be logged and investigated.

Incident Logging

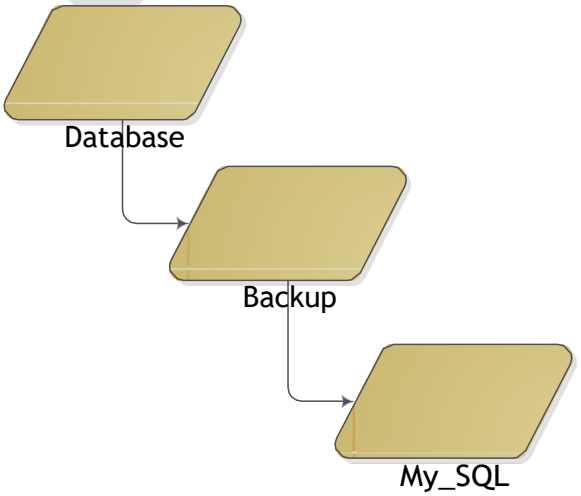
All incidents should be fully logged and time stamped regardless of how they are raised. All relevant information relating to the nature of the incident must be logged. This is to ensure a historical record is maintained and the incident can be referred to by all resolver groups. Information that is needed for each incident:

- Unique reference number (automatically assigned by ticketing tool)
- Incident Categorisation
- Incident Impact
- Incident Urgency
- Incident Prioritisation
- Name/ID of user reporting the incident
- Method of Notification
- Description
- Related Configuration Item

Incident Categorisation

Part of the initial logging must include incident categorisation. It is vitally important that categories are assigned as accurately as possible as these will be used to identify incident frequency and establish trends for use in Problem Management and other ITSM activities.

A multi-level categorisation system is used to assist in ensuring incidents are categorised accurately. An example of this is show in the below figure.



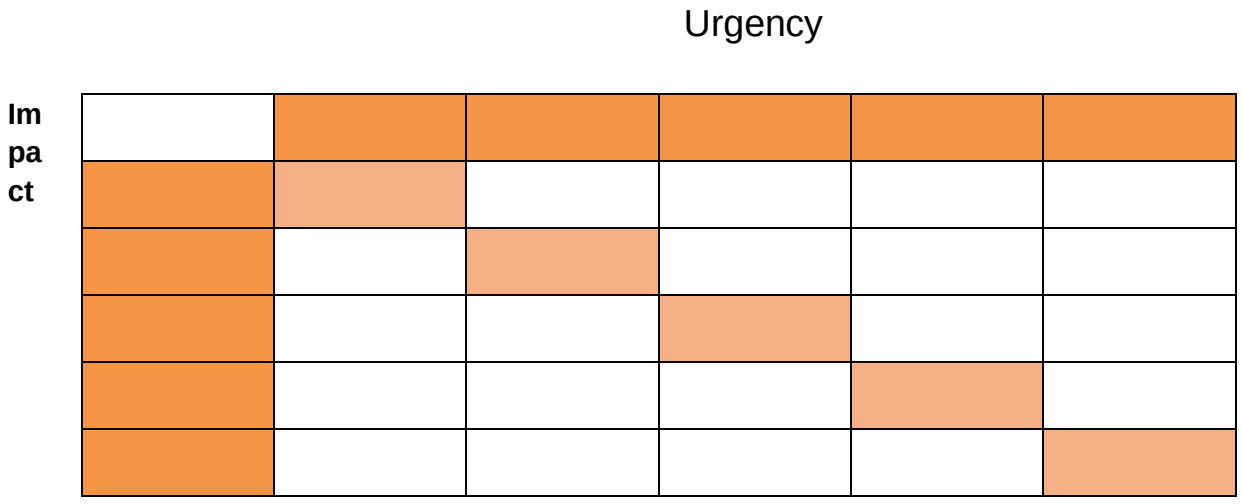
Note: Sometimes the detail available at the time an incident is logged may be incomplete, misleading or incorrect. It is therefore important that the categorisation of an incident is checked and if necessary updated, at closure time.

IM1.3 Request Fulfilment IM1.3 Request Fulfilment

The check for Service Requests in this process does not imply that Service Requests are incidents. This is a simple recognition of the fact that Service Requests are sometimes incorrectly logged as incidents. This check will detect any such requests and ensure they are passed to the Request Fulfilment process.

IM1.4 Incident Prioritisation

An important aspect of incident logging is to assign an appropriate priority. Priorities are determined by taking into account both the urgency and level of impact the incident is causing. A visual representation of how these elements are combined to derive an overall priority can be found in the following matrix:



It should be noted that an incident's priority may be dynamic. Circumstances may change or greater understanding of the issue is achieved, that will require the priority to be altered to reflect the new situation.

Note: Priorities vary depending on customer agreements, as set out in their respective Terms of Reference documents. The Service Desk tool is used to assign target resolution times to incidents based on the customer impact and priority assigned.

IM1.5 Hierarchal Escalation

Once an Incident has been prioritised, the Service Desk will determine if it needs hierarchal escalation. The reasons an incident will need hierarchal escalation are:

- Where the customer has requested that the incident be escalated
- If the Service Desk consultant determines that the incident is or may significantly impact the customers' ability to operate
- If a single issue is effecting more than one customer

Once it has been determined that hierarchal escalation is required, the Service Desk consultant will initiate the Escalation Procedure. For further details on the Escalation Procedure see *Section 3.3* of this response.

IM1.6 Service Desk P1 Management

The Service Desk is responsible for the management of all Priority 1 incidents. The service desk is required to ensure that The Customer is kept regularly updated on the progress of any incident, ensure that a resolver is assigned and working on the incident at all times, and that the incident record is updated with all relevant information:

- **Communication**: The Service Desk will agree a form and frequency of updates to the customer. Communication to the customer can be performed by both the Service Desk or Resolver Group, it is the Service Desk's responsibility to ensure it takes place at the agreed times.
- **Incident Investigation**: The Service Desk must ensure that there is a consultant assigned and working on the incident at all times. Incidents must be warm transferred between consultants and the Incident record updated with these details.
- **Incident Record:** The incident record is an auditable record of all actions relating to the incident and vital for the completion of Root Cause Analysis. The Service Desk will ensure it is kept up to date with all related details. The Incident Record will be updated by the Service Desk and Resolver Groups working on the incident.

If the Service Desk experience any difficulty with these tasks, they will escalate immediately via the Supplier management structure.

IM1.7 Escalation Incident Procedure

Details on the major incident procedure can be found in the response to *3.3.10 – Escalation Routes*.

IM1.8 Initial Diagnosis

Initial Diagnosis will be carried out by the Resolver Group assigned to the incident. Were possible, this should be done with the user still on the phone, to allow for early and accurate diagnosis. As soon as it becomes clear that the assigned consultant cannot resolve the incident, or the incident is in danger of breaching its SLA, the incident must be escalated along the functional escalation path for further support.

IM1.9 Functional Escalation

As soon as it becomes clear that the assigned consultant is unable to resolve the incident the incident record must be immediately updated and then passed to the appropriate technical team. The incident should be immediately escalated if the assigned consultant believes the incident requires deeper technical knowledge or the incident is in danger of breaching SLA.

IM1.10 Investigation & Diagnosis

The incident record should be updated with all investigation and diagnosis activities carried out by resolver groups. Investigation actions include:

- Establish exactly what has gone wrong
- Understand the chronological order of events
- Identify any events that could have triggered the incident
- Search previous incident records and knowledge base for relevant and useful information.

Note: Where possible, investigation and diagnosis activities are performed in parallel. Valuable time can be lost if these activities are performed serially.

IM1.11 Resolution and Recovery

When a resolution has been identified it should be tested and applied. Resolve actions may vary but can include:

- Requesting the user to undertake an action
- The Service Desk implementing a resolution centrally or remotely
- Resolver Groups carrying out recovery actions
- Third party supplier being contacted and requested to resolve fault

When a resolution has been found, sufficient testing should take place to ensure the recovery action is complete and the service has been fully restored.

IM1.12 Customer Resolution Confirmation

For incidents that have been reported by customers, the customer will be requested to confirm the resolution has been successful. These incidents should only be closed after the customer has confirmed the issue has been resolved. If a customer fails to respond to a resolution confirmation request the incident will be closed after an agreed time. The customer will be notified of the incident closure. If the customer states the issue has not been resolved the incident will return to the resolver group to determine if further escalation is required. The incident will then follow the ‘investigate and resolve’ steps before going back to the customer for approval.

IM1.13 Root Cause Analysis

For major incidents, the incident record will be kept open so that root cause analysis can be

carried out. This will only be done after the incident has been resolved, to ensure resolution SLA targets are not impacted. The purpose of carrying out root cause analysis at this is point is to verify that the underlying cause of the incident has been identified and corrective actions have taken place. The outcome of the root cause analysis is a report that can be shared with The Customer.

Information security management will review all RCAs to ensure the confidentiality, integrity and availability of an organization's information, data and IT services has not been compromised.

IM1.14 Incident Closure

The resolver group should check the incident is fully resolved and that the user is satisfied and willing to agree the incident can be closed. The following checks should also be done:

- Incident Documentation – follow up on any outstanding details and ensure the incident record is fully up to date
- Recurring Problem – determine whether it is likely that the incident could recur and if any preventative action is required. Problem Manager should be engaged to advise on this matter
- Formal Closure – To formally close the incident. In some cases this will be done automatically after the incident has been resolved. The timeframe for this is set by the support tool.

Despite all adequate care, there will be occasions when incidents recur even though they have been formally closed. If incidents recur more than 7 days after the incident has been resolved and the incident has been formally closed, a new incident must be raised, but this can be linked to the previous incident.

For evaluation purposes we have included a copy of our Incident Management Process, which includes our Major Incident Procedure. This is included as a separate PDF document - *Appendix E - V1 - MSP Incident Management Process.* An *Example Incident Report* is included as *Appendix G*.

Service Restored

On investigation of the problem, service may be restored via a known workaround or a temporary fix put in place, if one exists. (Note: a workaround may not always be available).

Investigation and diagnosis to a permanent fix of the problem will continue once service has been restored.

Testing

Testing will be completed (in line with the 1-Test process as detailed in response to *3.7.4 – Testing & Assurance*) to validate and verify that the fix works as expected.

Any new issues not introduced by the defined incident/problem, discovered during testing, will be logged and treated as new issues. The issues will not be made a part of the current change. The issues may or may not be released as part of the current scheduled release.

User Acceptance Testing (UAT)

The Customer owns the UAT activity, and therefore can prepare and execute any tests you deem appropriate. The Supplier team can assist in the development of these tests or with review and validation.

- It is the responsibility of The Customer to perform all UAT testing
- Any new issues not introduced by the defined change, discovered during UAT testing will be logged and treated as new issues. The issues will not be made part of the current change. The issues may or may not be released as part of the current scheduled release.
- UAT testing must be signed off by The Customer.

Release to Live

- All releases will be done in accordance with our Release Management process. Our Release Management process is included in the appendices at *Appendix B - V1 - MSP Release Management Policy* (separate PDF document attached to submission)

Updating The Buyer

The Customer can access the status of their incident at any time by logging into the Supplier Customer Portal at https://my.The Supplier.com/

Regular reports will be sent to The Customer reporting on service level performance. We will also liaise with 3rd parties where necessary when responding to incidents raised, managing the end-to-end process to resolution ensuring all parties are keep informed accordingly.

Change Control

All Incidents and Problems that require a change to a production system must first receive approval from The Customer and the Supplier Change Advisory Board (CAB), prior to implementation.

Major Incidents

If an incident is an Emergency Incident (P1 issue), it may not be possible to get a document in advance of deploying a fix.

The Major Incident (Priority 1) process addresses critical incidents that require a response above and beyond that provided by the normal incident process. Such incidents may have a major impact on the ability to sustain operations or effectively run the business. Although these incidents still follow the normal incident life cycle, the major incident procedure provides the increased coordination, escalation, communication, and resources that these high-priority events require.

A Major Incident is an unplanned or temporary interruption of service with severe negative consequences. Examples:

- Outages involving core infrastructure equipment/services that affect a signification customer base
- Total loss or failure of a service/function at a critical time in a customer's business calendar.
- Total or significantly impaired loss of a customer system which cannot be resolved within normal timeframes.
- Significant customer incident which requires support input from multiple teams/skills/resources.

This process is controlled by the major incident manager. The major incident manager will assemble an incident resolution team and team membership will vary according to the demands of the incident. We have covered in our response to *3.4.8 - Major Incident (P1) Management*.

1.4.4 Service Desk Portal

The Supplier's Service Desk will act as the primary point of contact for all The Customer incidents. The Service Desk triage incidents report through monitoring alerts, phone, and email. The Customer can also log issues via the Supplier customer portal at https://my.The Supplier.com/ and incidents can also be auto generated where automated alerting is in use, as a result of an alert being received.

For convenience, The Supplier's web portal provides a facility to allow customers to search the LANDesk system using the customer's reference number. The Customer can access the status of their incident at any time by logging into the Supplier Customer Portal at https://my.The Supplier.com/

The Self Service Portal will allow The Customer to easily track all issues you have raised with us that are open or closed. It also allows you to raise new issues with the Service Desk team within seconds.

We will also provide The Customer with a secure knowledge base to support your infrastructure estate. We will populate our knowledge base with the information required to support the infrastructure and associated systems/services. There will be technical information (such as remote connection details, servers details, ip addresses, source code details) and functional and operation information such as the FRD, "how to" procedures, known issues, scheduled processes. This will ensure that any recurring or repetitive issues and their associated solutions are quickly highlighted and are able to be actioned.

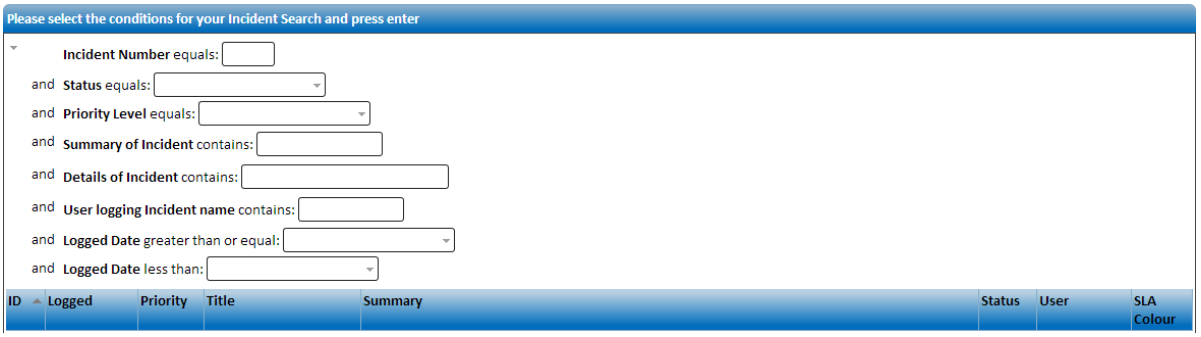
To access the site you must first be setup with permissions to raise calls with The Supplier's call ticketing system, this can be confirmed by the Supplier Service Delivery Manager assigned The Customer, or you can request access by emailing the servicedesk@The Supplier.com . The Service Desk team will then provide you with your username and password to logon to the system. The Self Service Portal is located at https://my.The Supplier.com/

Once you have logged in the customer portal you will be able to see all the current incidents and changes you have open with The Supplier. You will also have an option to switch between multiple projects/contracts which are open.

The new incident page allows you to raise issues for the attention of the Service Desk and your support team. From here you can add a summary and a description detailing the issue. You can change the level of business impact which the issue is having within your organisation if it differs from the default 4-Moderate. After this is filled in you can then “save and close” the page.

You will receive a reference number to follow up with your call if needed.

There are two searches available within the Self Service Portal, one for incidents and another for changes. The searches allow you to review open and closed calls raised with The Supplier. You will be presented with several search attributes to use when locating specific Incidents and Changes.



In addition to this web-based provision, automated reports can be sent by email directly to a specified distribution list of The Customer stakeholders, with all relevant service figures at agreed intervals (daily, weekly, monthly or on request) throughout the life of the agreed services.

1.4.5 Service Desk Metrics

As part of the managed service agreement, The Supplier will provide a monthly service report to The Customer incorporating detailed information regarding the performance of the service desk in responding to and resolving calls / tickets. The Supplier can also provide The Customer with the raw data used to produce the reports for further analysis by The Customer should this be required.

Further to the information above, included in the monthly service report (and also published to the collaboration site) will be Service Availability and Capacity information and KPI data as follows:

Service Availability KPI's:

- % Service Available
- % Service Unavailable
- Duration of downtime in service
- Frequency of failure
- Impact of failure
    - On end user
    - On business transaction process/operations

Capacity KPI's:

- Percentage reduction in over-capacity of IT, e.g. Storage
- Number of Capacity Related Incidents/Problems
- Percentage reduction in the number of Capacity-related incidents/problems
- Percentage of changes (marked by Change Management as affecting capacity) assessed for their impact on the capacity and performance
- Percentage of SLA breaches caused by insufficient capacity

- Percentage change in the number of proactive problem resolutions initiated by capacity process
- Percentage accuracy of forecasts of resources utilisation/workloads
- Cost of spend of unplanned purchases on Capacity.

The reporting period can be specified in accordance with monthly service management review meeting requirements. The Supplier will provide this report one week prior to the scheduled meetings, to allow for discussion points, agenda setting, and any actions that are required for discussion at the review meetings.

In addition to the monthly service management reporting, The Supplier will also produce a quarterly trend report (including supporting narrative) which highlights the key themes, trends, issues, and risks that have developed in the managed service provision throughout the preceding quarter. We will provide this to The Customer in advance of the quarterly Supplier Strategic Review Board, and will discuss the content with attendees at the review board.

The LanDesk reporting suite facilitates the inclusion of any other tailored reporting requirements specified by The Customer, in accordance with changing service/business needs. This may include areas such as Problem Management Report (example of these stats included in response to *Section 3.3.5 – Problem Management*) which we will provide to The Customer at a frequency to be agreed (typically monthly). This will include:

- The status of all Problems raised during the period (e.g. Draft, Assigned, In Progress, Resolved, Closed, Closed etc.)
- Number and % of New Problems Opened and Closed
- Number and % of Problems Opened and Closed by Priority
- Number of Problems Opened and Closed by Assignee Group
- Trend of status history, e.g. last 3 periods
- Number and status of all Problems since Year start
- Aged Analysis of Open Problems by Team
- Aged Analysis of Open Problems by Priority
- Detail list of all Problems assigned since start of period.

An example service management report has been included in *Appendix A - Monthly Report Sample* (separate PDF document attached to submission). We have also included *Appendix 7.5 - Evidence of Response Times for Existing Customers.* This has been included to illustrate our excellence in meeting and exceeding our Incident Response time SLA's.

1.4.6 Major Incident (P1) Management

The Supplier's Managed Services Practice has 250 highly qualified staff working in first, second and third level support teams. The teams and team members work closely together and readily share information and help each other with technical issues, ensuring a customer first approach with the goal to resolve any issues as quickly and effectively as possible.

When a priority 1 issue is reported, the service management tool automatically emails all of the technical teams involved in supporting the customer and the management team. The second level support team will commence their investigation as soon as a priority 1 issue email is received.

Non-priority 1 issues that cannot be resolved by the first level support team are passed to the second level support team for investigation, typically in under an hour. The second level support team members will draw on the expertise of the third level staff as required. Ownership of highly complicated issues will be passed to the third level support team for resolution.

The Major Incident (Priority 1) process addresses critical incidents that require a response above and beyond that provided by the normal incident process. Such incidents may have a major impact on the ability to sustain operations or effectively run the business. Although these incidents still follow the normal incident life cycle (as detailed in our response to *Section 3.4.4*), the major incident procedure provides the increased coordination, escalation, communication, and resources that these high-priority events require.

A Major Incident is an unplanned or temporary interruption of service with severe negative consequences. Examples may include:

- Outages involving core services that affect a signification user base
- Total loss or failure of a service/function at a critical time in The Customer's business calendar
- Total or significantly impaired loss of a The Customer system which cannot be resolved within normal timeframes
- Significant incident which requires support input from multiple teams/skills/resources.

This process is controlled by the major incident manager. The major incident manager will assemble an incident resolution team, and team membership will vary according to the demands of the incident.

- The call is logged as a P1 to the Supplier Service Desk
- The The Customer team is informed of P1 situation via a ticket an email notification and/or a call
- A P1 Notification Email will be sent out to the The Customer P1 email distribution list
- The The Customer support team investigates the issue and provides the The Customer contact with an initial response
- The Major Incident Process is initiated if the P1 is not resolved within 30 minutes. We will invoke this process sooner if they deem it appropriate
- The Major Incident Manger is appointed who will take ownership and manage the incident to resolution The Major Incident Manager will involve the Incident Resolver Team for an initial meeting to determine:
    - What has happened?

- What is the Impact to The Customer?
- Agree who will do what (for a technical fix and for communication)
- Incident Resolver Team will concentrate on the technical resolution:
  - Determine the cause
  - Identify & implement fix
  - Identify workaround
  - Provide updates on what is being done
- Communication will run in parallel with the technical work and will be coordinated by the Major Incident Manager
- Technical consultant to write up a root cause analysis (RCA) of the problem identifying follow on actions where required
- Hold an end of incident review

All reports associated with any major incident will be completed and supplied to its IT Operations & Service Manager within five working days of the incident's resolution. For evaluation purposes we have included a copy of our Incident Management Process, which includes our Major Incident Procedure. This is included as a separate PDF document - *Appendix E - V1 - MSP Incident Management Process.*

Root Cause Analysis Root Cause Analysis

A root cause analysis (RCA) document is completed for all priority 1 incidents once service is resumed to ensure that the underlying cause of the incident/problem is identified and recommendations made on how to prevent a similar issue in the future.

- A root cause analysis document is completed and returned to the customer. (Note: An RCA will be completed for all P1's regardless of whether the issue is within or outside the control of The Supplier. An RCA for a problem that is outside the control of The Supplier will just mention where the problem was and any known information on the problem. It may not always be possible for The Supplier to determine the root cause in this case).
- All outstanding follow-on actions must be logged and referenced in the root cause analysis document.
- The RCA must be reviewed and signed off by the Services Manager/Managed Services Manager.
- The follow-on actions must be linked to the P1 call.
- The P1 will only be closed after all follow on actions have been completed by the Service Desk Manager.
- All reports within the month will be an agenda item on each month service review.

We have provided a sample Root Cause Analysis form in *Appendix 6.4* for review.

Trend Analysis

The Supplier team leads will perform a review and trend analysis on incidents and problems logged during the reporting period to help identify areas where there may be an increasing trend for a particular type of incident. Incident analysis can help in both reactive and proactive problem management.

Trends that the consultant will be analysing include:

- Is there an increase in the number of incidents of a particular type?
- Is there an increase in the number of incidents on a particular area of functionality?
- How many high priority incidents are logged?
- What is the possibility of the same problem occurring elsewhere (i.e. Is there a possibility that the problem we had on server 1 will also occur on server 2?)

An examination of these trends can help us to identify the following:

- Need for process improvement
- Need for improved documentation

Recommendation to investigate and implement changes to eliminate the root cause of one or multiple incidents.

The Supplier will provide all trend analysis for review at the quarterly Strategic Supplier Review Board.

1.4.7 Service Delivery Manager

The Service Delivery Manager for the Legal Ombudsman will be Adrian. Adrian will be The Customer's advocate within The Supplier and is the first point of escalation for any issues relating to the Managed Service provision. Adrian has a proven track record of working with many Public Sector customers such as the Rural Payment Agency, Student Loans Company, the British Library and Aberdeenshire Council

Indeed, Adrian has been acting as Service Delivery Manager for The Supplier's existing CMS Managed Service with The Customer for the past 15 months and therefore is extremely familiar with the organisation, the key stakeholders, the technology landscape, The Customer's operational procedures, but also the processes that The Supplier currently operate under for that contract.

Should the Supplier be successful under this procurement, we propose to extend Bruno's SDM role to cover both the existing CMS Managed Service, and the new Infrastructure Managed Service. Whilst these will be 2 separate contracts, the operational service delivery from the SDM and service desk will be virtually the same, and we believe this represents some distinct benefits to The Customer in the effective running of your operation, particularly around your systems and technology:

- Reduced ramp-up and transition time. As The Supplier staff are already familiar with The Customer, and the existing technology estate, this will result in a shorter transition and quicker time to mobilise as the initial discovery phase will be reduced when starting the infrastructure build activities
- One point of contact for all IT related issues across The Customer, whether that is in applications, database, infrastructure, networking
- Already proven and effective way of working between The Supplier and The Customer, easily extended to cover the infrastructure requirements under this contract
- Efficiencies in incident analysis and resolution times. As incidents are not being worked on my multiple parties, The Supplier will be able to more quickly identify the root cause of issues / incidents across the The Customer estate, leading to a quicker resolution time for The Customer, and any affected users
- Less stakeholders for The Customer to engage with, which leads to reduced overhead for The Customer staff relating to governance, supplier meetings, monthly / quarterly service meetings, billing, etc. By working with a more consolidated operating model and reduced number of suppliers, this should prove to me more cost effective for The Customer over the course of the contract.

Notwithstanding the above, The Supplier believe in a customer-centric service model for all our managed service contracts to ensure the effective provision of all contracted services and that any issues are dealt with in a timely and professional manner. At the heart of this is our Service Delivery Manager, and for The Customer, Bruno's responsibilities will include:

- Liaise with The Customer IT Operations and Service Manager
- To perform the role of an advocate and champion for The Customer within The Supplier
- Ensure an ISO 20000 compliant service is being delivered to The Customer:
    - operationally manage the provision of all contracted services
    - coordinate the involvement of other MSP staff involved in delivering the day to day service
    - liaising with any designated person(s) responsible for coordinating the delivery of non BAU (business as usual) change

- Act as escalation point for The Customer
- Create and record links to key stakeholders within The Customer
- Conduct Service Review Meetings with Key Project Sponsors and/or Vendor Manager
- Agree, Measure and Manage Project Specific KPI's and Conditions of Satisfaction with The Customer
- Assist the Supplier team in resolving issues for The Customer
- Ensure we deliver excellent service (as measured by customer satisfaction surveys)
- Identify ways in which we can improve our service
- Assist The Customer IT Management in the delivery of the overall service to The Customer's end users
- Ensure Value Added activities from the Supplier Service Catalogue are being delivered
- To ensure we are meeting and indeed exceeding our commitments to continual service improvement
- To act as a liaison with product vendors such as Microsoft when appropriate.

Bruno will agree conditions of satisfaction with The Customer on a quarterly basis. Conditions of Satisfaction are KPIs that The Customer indicate would merit a high satisfaction rating if delivered. The conditions of satisfaction are agreed between the Service Delivery Manager and The Customer nominee(s).

On a quarterly basis we will issue a standardised survey to The Customer to measure your levels of satisfaction across a number of areas. We will ask you to specifically take into account our performance with regard to the delivery of the specific Conditions of Satisfactions agreed for the previous quarter. In this way satisfaction ratings are aligned with specific goals agreed with The Customer.

Based on individual survey responses the appropriate action will be taken with regard to Service Improvement initiatives, complaints actioning and required communication with service delivery personnel.

1.4.8 Account Management & Direction

The Service Delivery Manager is accountable for the delivery of the contracted services to The Customer, including customer satisfaction scores and will work with The Customer to set conditions of satisfaction; initiatives set on a quarterly basis set by the customer to continuously drive higher and higher levels of service.

The Service Delivery Manager will work with the support teams to ensure that the conditions of satisfaction are met. This focus on continuous improvement drives a very high standard of service and as a result reduces the number of escalations required to almost zero. Once an incident is logged, it may be escalated from its default priority to a higher level.

The Supplier will assign an Account Manager to The Customer who will act as the point of escalation for the Head of IT at The Customer. The Account Manager will be senior to and have authority over both the Service Delivery Manager and any person given responsibility for coordinating non-BAU change.

Adrian Buckley will act as Account Manager for The Customer. As with the SDM, Adrian has been working with The Customer over the past 10 months as Account Manager for The Supplier's existing CMS Managed Service. Should The Supplier be successful under this procurement, we propose to extend Adrian's role to cover both the existing CMS Managed Service, and the new Infrastructure Managed Service.

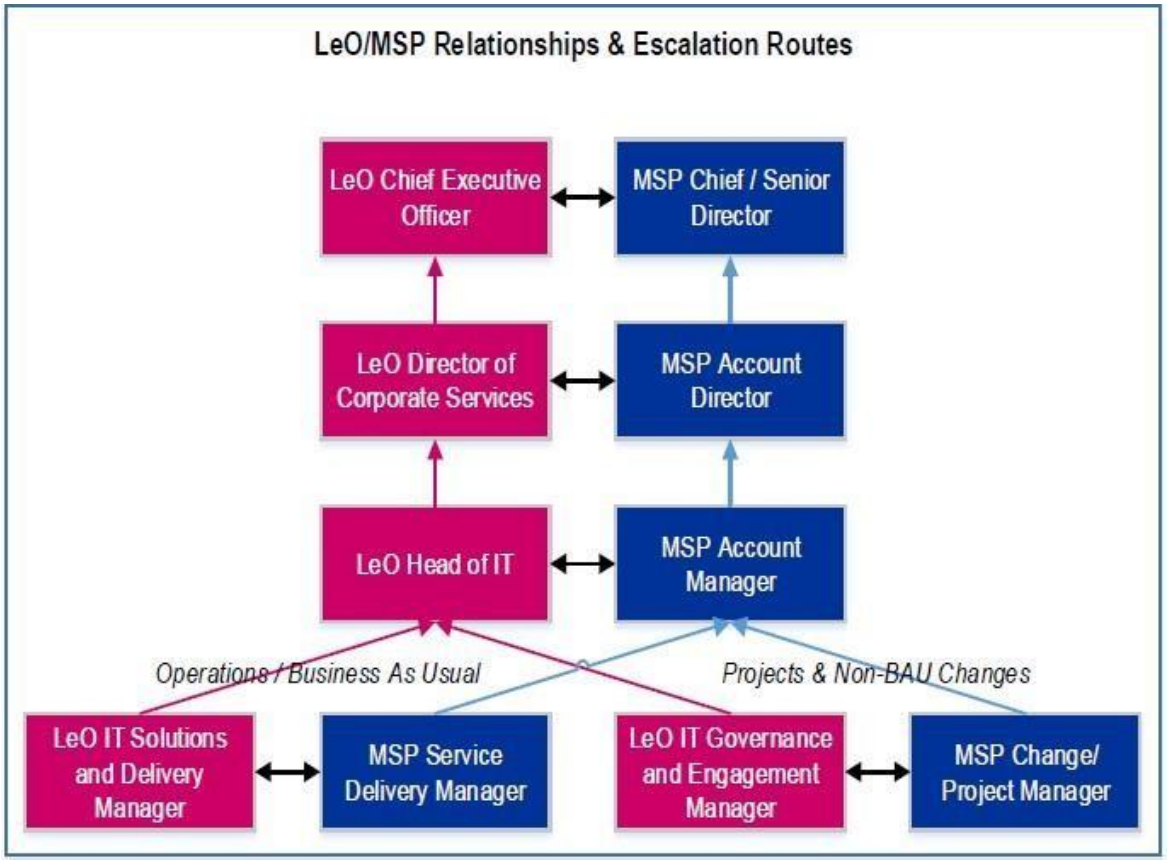
This will ensure continuity for The Customer in terms of key The Supplier personnel assigned to the contract. Both Bruno and Adrian will continue to work closely to ensure effective service delivery, adherence with contractual commitments, commercial management, and ongoing service improvement. With this existing familiarity with the The Customer operation and key personnel, we believe this provides The Customer with an experienced team from which to engage with and escalate where necessary.

In order to escalate an issue to a higher priority level, The Customer will phone the Service Desk with your Service Desk reference number and ask that the issue be escalated and give the reasons for the change. You may also wish to specify the frequency with which you want a progress update.

In terms of aligning the Supplier personnel to the The Customer/MSP Relationships & Escalation Routes below, this is as follows:

- MSP Chief / Senior Director - Joe O'Brien
- MSP Account Director - Joe O'Brien
- MSP Account Manager- Adrian Buckley
- MSP Service Delivery Manager - Bruno Almeida
- MSP Change/Project Manager - to be determined by on each project requirement

The Supplier can also include our Chief Operating Officer, Tom O'Connor, as a further escalation point if required, as the Supplier directors, in line with our *Customer First* value, make themselves available as required for customers particularly in the case of any required escalation.



1.4.9 Escalation Routes

We have reviewed The Customer's suggested "Relationships & Escalation Routes", and in principle this matches The Supplier's Managed Service provision. It also aligns to the existing structure that we operate for our current CMS Managed Service contract with The Customer. Therefore, given that the key stakeholders on the Supplier side will remain the same, this will prove to be a seamless extension of that structure to cover the specific requirements covered under the Infrastructure Managed Service contract. Established relationships at all levels will remain and escalation routes will operate as they currently do, where we consistently demonstrate timely and helpful action in the event of an issue arising in either organisation.

The Supplier's escalation processes are included in the scope of the company's ISO20000 certification. The process includes escalations:

- From customers relating to an incident
- From customers relating to broader service issues
- Within The Supplier to address priority issues
- To third party providers where critical incidents are passed to third parties

ITIL defines two distinct types of escalation:

1. Functional escalation occurs where an incident necessitates a different skill set and must be handed over to a separate function (or team) for resolution.
2. Hierarchical resolution occurs where an incident is of such a serious nature that it merits more attention from higher levels of management, or that it is not being addressed within acceptable timeframes and further management intervention is required to ensure that it is addressed.

While we endeavour to ensure that all our consultants have appropriate skills to enable them to address most issues that may arise, there are occasions when they may need to call on additional resources, with specific skills or knowledge to resolve an issue. This happens seamlessly and our Service Desk tool supports the reallocation of incidents in this way.

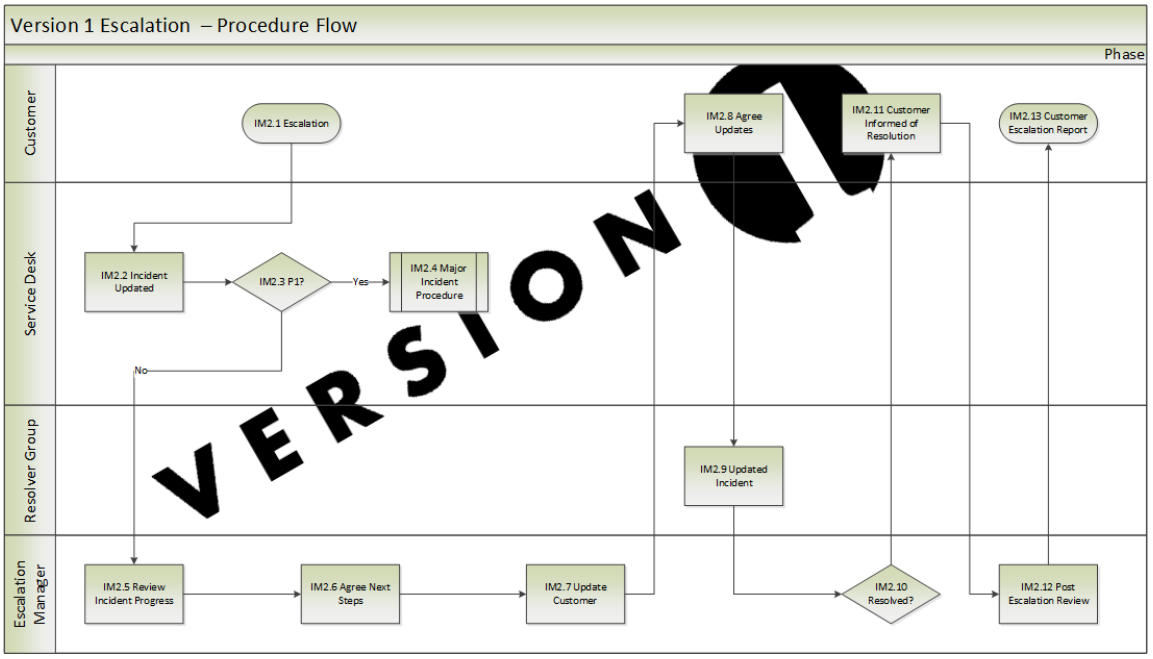
Where an incident is at risk of breaching agreed SLAs, an automatic notification is generated, and your SDM will be notified. The SDM will work with the support team, and with you, to ensure that appropriate additional resources are assigned if required, and that the incident can be resolved to your satisfaction.

Priority 1 incidents are automatically notified to your SDM, and the Managed Services Practice head as soon as they are logged. We will work with you to determine the best way to integrate these processes into your own incident management processes.

Once an incident is logged with our Service Desk it may be escalated from its default priority of P4 to a higher level at any point and for any reason.

If for any reason The Customer wish to escalate an issue to a higher priority, phone the Service Desk with your Service Desk tag number and ask that the issue be escalated and give the reason for the change. You may also wish to specify the frequency with which you want a progress update.

The escalation swim lane diagram is applied to all customer escalations – The Customer's responsibilities are shown in the Customer lane.



The steps in the Escalation Procedure are

- IM2.1 - Procedure is initiated by the customer contacting the Service Desk, or notification coming from Opsview monitoring tool
- IM2.2 - Service Desk updates the Incident record with details of customer escalation, and communicates the outage to the customer in the event it has not yet been reported
- IM2.3 - Service Desk check if the incident is a priority 1
- IM2.4 - If the incident is priority 1 it will be handled under the Major Incident Procedure. An escalation manager is assigned, this will be the Service Desk Manager unless otherwise agreed
- IM2.5 - Escalation manager reviews the progress of the incidents and contacts the resolver team working on the incident for an updated
- IM2.6 - Next steps agreed with the Resolver Team. This will include next action to be taken and time of next update
- IM2.7 - Escalation manager updates the Customer
- IM2.8 - Customer receives update and agrees update schedule
- IM2.9 - Resolver Group update Incident record with details of incident investigation
- IM2.10 - Escalation manager checks incident for updates and informs customer once the incident has been resolved
- IM2.11 - Customer reviews and confirms resolution
- IM2.12 - The Escalation manager will begin and Post Escalation Review
- IM2.13 - The outcome of the post escalation review will be a report that is then shared with the customer.

1.4.10 Service Reporting & Reviews

Monthly service review meetings are part of The Supplier's standard managed service provision and we would be pleased to adopt this for the The Customer Infrastructure Managed Service contract and the proposed Supplier Service

Management Forums. The meetings take place between The Customer representatives, The Supplier's Service Delivery Manager and representatives of the Supplier Infrastructure Managed Service team.

During the implementation/transition stage of the Infrastructure Managed Service, The Supplier recommends a weekly meeting takes place between The Customer and the Supplier team running the transition. Thereafter, the frequency would move to the monthly Supplier Service Management Forums as defined by The Customer, although should weekly meetings be required beyond the completion of transition they should continue beyond that period upon agreement by both parties.

The Supplier SDM will propose an agenda for The Customer to review and amend in advance of the monthly meeting (service management forum). The agenda will allow the SDM to ensure that the appropriate The Supplier staff attend the forum and provide input where required. The agenda typically covers performance against service levels, service performance and progress against the actions agreed at the last meeting. At a minimum it will include agenda items to:

- review the supplier's performance report for the last period
- agree any service credits that may be due
- discuss incident reports and any proposed preventative measures
- discuss progress on problems and items in the Continuous Service Improvement Plan (CSIP)
- escalate issues that cannot be resolved within the forum to either senior individuals from The Customer and the supplier or the Strategic Review Board
- note any significant business matters that may impact on service
- review the arrangements for changes being accepted into service

The Supplier can also conduct joint service reviews where required to include other associated third parties. We adopt this approach this for a number of enterprise customers where there may be a complex, multiple supplier eco- system.

On a quarterly basis the Supplier Strategic Review Board will be attended by the Supplier Account Manager and Account Director, and when required the SDM. The quarterly meeting is in line with The Supplier's standard Managed Service provision and is used to review the past quarter and assess The Customer's level of satisfaction with the service quality and agree a set of "conditions of satisfaction" for the coming quarter. The conditions of satisfaction are a set of objectives that, when delivered, will improve the quality of the service for The Customer. Conditions of satisfaction are set regardless of how high the satisfaction level is - The Supplier holds a view that there is always room for improvement.

In addition to a focus around the service provision, additional agenda items will be to:

- review performance trends and key actions from the preceding period
- share intelligence on the public and legal sectors, and their own stance
- discuss and attempt to reach agreement on any escalated issues
- consider any commercial or contractual issues that have arisen or are due

In relation to the monthly and quarterly supplier meetings above, this structure is very similar to governance model operated in The Supplier's existing CMS Managed Service. Should The Supplier be successful under this procurement we would be pleased to discuss merging/extending these meetings with the Infrastructure governance as we believe, given the joined up nature of both operational and technical services, there would be benefit to both The Supplier and The Customer in combining the governance models.

In addition to the scheduled supplier meetings, The Supplier recognise there is an ongoing need to be involved in Technical Assurance Panel and Delivery Board when input is required by our various technical teams. We are familiar with how these forums are run within The Customer having been involved in recent change activities and ongoing project delivery related to the CMS, and are pleased to see this governance model extending into the infrastructure management. We will also provide appropriate technical expertise in writing for consideration by The Customer's own Change Advisory Board (CAB) as and when required.

Under our existing CMS Managed Service with The Customer, The Supplier operates its own Change Advisory Board. All changes to any production system must be approved by the CAB, which typically meets on a weekly basis. An Emergency CAB can be called in an emergency situation. We would expect to extend this approach to the Infrastructure Managed Service should we be successful, and we have included further details on this in our response to *Section 3.7.2 – Change/Project Governance*.

1.4.11 Continuous Improvement

We note The Customer's clear statement to move towards an integrated and coherent infrastructure, delivered by a smaller range of suppliers than you currently have. The Supplier already provides an ITIL Managed Service for the The Customer CMS, and throughout the response to *Section 3.4.1 – Take On & Exit* we have detailed how we would transition the The Customer infrastructure service into The Supplier managed support, and then migrate the full ICT estate to a new Azure environment in a controlled and phased basis. We have highlighted potential risks to The Customer, and explained how we will mitigate these risks to ensure service continuity and no disruption to users as we assume responsibility for the whole ICT estate.

We firmly believe, and have demonstrated throughout this response, that with The Supplier providing the existing CMS support and also the infrastructure managed service, The Customer will move to a simpler operating model, more effective service management right across the organisation, less overheads internally, and most importantly delivered by a proven supplier with a detailed understanding of The Customer who can add value from the outset, whilst providing the long stability improvements that the organisation requires.

At The Supplier, we fully embrace Continuous Service Improvement as a core tenant of our Managed Service offering. Our commitment to a CSIP (Continuous Service Improvement Pro-

gramme) is such that we incorporate it into our Managed Service from the outset of our engagement with The Customer. This means that The Customer will start reaping the benefits of our proactive approach straightaway rather than waiting for such initiatives to commence further into the contract.

Our transition process will include the formation of a CSIP and will seek to identify both “quick wins”, i.e. initiatives that can be expedited and bring improvements in areas such as system or operational efficiency, and strategic initiatives. We have noted The Customer’s plan to allocate a number of call off days annually / monthly to service improvements and enhancements. We have a proven track record in delivering service improvements across our Managed Service engagements including during the take-on phase with examples such as:

- Department of Transport, Tourism & Sport: streamlined monitoring & checking processes associated with the National Vehicle Driver File case management system to reduce effort for Technical Database Specialist activities by over 90 days per annum with savings passed back to the Department
- SSE: identified a database related issue affecting the performance of their Billing and Customer Information System and outlined system changes required to resolve the issue thereby resulting in a smoother support transition and greater customer satisfaction
- Musgrave Group: reduced weekly price upload ETL process of their Data Warehouse & Pricing System from 52 hours to 12 minutes. Previously it had been ‘accepted’ that the incumbent team of independent contractors could not improve the process any further.

This commitment to ITIL Continuous Service Improvement (CSI) is driven by the culture of ‘business-led’ service management. There are two strands to The Supplier CSI efforts:

1. CSI for internal The Supplier Service Management processes, benefiting our customers by the tuning of processes for optimum effectiveness, efficiency, and flexibility. These efforts are driven into our own operations for delivering high quality services to all customers

2. CSI for the business specific services we deliver to our customers, and in this case the services delivered to The Customer as key Managed Service customer

The first aspect The Supplier operationally work towards is ‘business-as-usual’ operation, as a commitment in accordance to our core values of drive and customer first, and also as a basic requirement for our ISO20000 accreditation. For The Customer, this will focus on ensuring the investment you have made up to this point can be realised as best as possible and looking at measures to improve the stability and performance on the The Customer infrastructure, among other things.

The second aspect is one that directly influences the Supplier service commitment to you and your unique business requirements. Throughout the partnership with The Customer, The Supplier will continually provide advice and guidance on best approach, technology innovations and assist in the development of technology roadmaps with the goal of ensuring the The Customer ICT environment is future-proofed and capable of keeping ahead of business demand.

The Supplier CSIP is focused on initiatives that can range from reducing operating costs to a business, to providing our customers with additional competitive edge – all with minimum risk. CSI is a constituent part of each of The Supplier ITIL processes, so that continual reviews take place in order to ensure they are fit for purpose. This is a standard tenet of ISO20000 accreditation requirements and is firmly embedded in our service delivery approach.

It must be noted that CSI takes place in different forms and on different scales. Some aspects are related to identifying smaller opportunities to drive out cost for The Customer by introducing economies of scale around processes and tasks. But, as solution providers, The Supplier may recommend larger strategic transformational programmes, introducing new technologies or solutions.

How this process takes shape is firstly through the Service Review meetings, continually measuring the service against agreed SLAs and proposing improvements through our own expertise, as well as feedback from The Customer on the overall provision of service in line with conditions of satisfaction.

Some examples of agenda items to help inform CSI we would be keen to discuss with you at Service Review meetings would be, but not limited to:

- What are the future business needs of The Customer in terms of capacity?
- Are there strategic business changes The Customer is undertaking in the next 6 months that The Supplier can ensure the IT provision will fully support?
- How have The Supplier as a provider, performed against call answering, incident, service request, problem and availability Service Levels? Should these be reviewed due to upcoming changes to business needs?
- Is The Customer happy with the overall service? What can The Supplier do to improve? (supported by periodic surveys)
- Can The Supplier offer other innovative ways to make the value of IT to the business more transparent?

The Supplier will maintain a CSI log of all requested and proposed service initiatives, which can be reviewed at each meeting to track progress. This log would be stored and maintained by The Supplier as an addendum to the Service Catalogue, and would be accessible to The Customer stakeholders as and when required.

The following are examples of CSI initiatives for one of our major infrastructure customers:

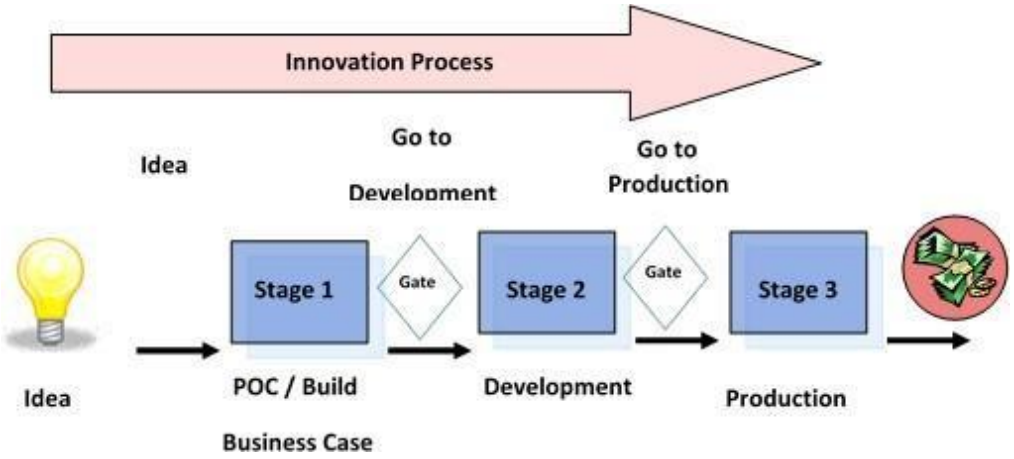
IPC	Category	Recommendation	Status
290829	Optimise Backups	Investigate use of snapshot backups	Implemented
300033	Auditing	Sylog Server on the OOB Network	Approved - Schedule
15587	Improve Usability and security	Link Solaris 11 accounts into AD for password authentication	Awaiting Review
2929871	Improve Security	Review of sudo rules for Solaris 10 servers migrated "as-is" from pre-prod	Awaiting Review
300750	Improve Security	Implement LAPS	Awaiting Review
2814908	Improve Usability	Install new HP 3PAR reporting console	Implemented
2823433	Improve RTO	Configure File Server replica to hold restore points to allow fail back to previous point in time	Approved - Schedule
310459	Improve RTO	Add iLO FQDNs to DNS	Implemented
300033	Improve Security	Integrate iLO with AD.	Implemented

303053	Improve Performance	Enable CSV Cache with Hyper-V.	Implemented
300037	Improve Availability	Replace existingg Cisco 4500 switches in Maynooth Office	Not Approved - Cost Benefit
290829	Improve RTO	On the T5240s, offsite recursive ZFS snapshots of root FS for bare metal restore purposes	Approved - Schedule
2811678	Improve Stability	Consider another provider for links between TC1 and TC2	Implemented

Based on our knowledge of working with The Customer, there are number of areas where The Supplier believe we can add further value and incorporate into our CSIP. This includes areas such as:

- Journey to cloud
  - More and more enterprise customers are “moving to the cloud”. The Supplier has been delivering and managing cloud solutions since 2009. We can safely accelerate the The Customer journey to the cloud across all your software solutions and help navigate the pitfalls.
- Online Services (including Verify.gov.uk)
  - The Supplier has implemented many online systems for Government customers, including the integration to Verify.gov.uk, the UK Government’s verification and authentication service introduced by Government Digital Service (GDS).
- Software Asset Management
  - Efficient Software Asset Managed Service can bring enhanced value to the The Customer software estate and help define strategic programs to increase this efficiency.
- Unified Communications
  - There are significant commercial, technical and productivity benefits to be gained by migrating from traditional PBX solutions to future proof IP Telephony.
- Enterprise Business Intelligence
  - The Customer manage large volumes of data across the operation, with limited reporting or business intelligence. Methods of utilising, analysing and sharing this data within The Customer and to third parties could bring improvements to The Customer for fairly low levels of investment.

As a value option designed to enhance the service offering of Continual Service Improvement The Supplier can offer to undertake, on a quarterly basis, an innovation workshop with a small group of The Customer Staff and The Supplier resources. Our innovation process is based upon Stage Gate, the best-practice standard for managing innovation excellence. This could be an exciting opportunity to mix multiple talents from across the business from Marketing, IT, and Customer Service. The process is designed to elicit ideas based upon specific criteria at each stage. The Supplier has created a set of templates to facilitate this process which are used for the purpose of governance by an Innovative Committee. This group filters the ideas and decides on the most innovative ideas, eliminating ideas at each stage, until one meets the required criteria to enhance.



The Supplier can mobilise the wider talent from our Technology Consulting Pool and Business Transformation practice groups to assess what value-add in business or technical terms can be provided to The Customer within the core services, as well as additional initiatives to be considered outside the core services scope.

The Supplier's business consultants are acknowledged experts in business transformation enablement, working closely with enterprise customers to effect significant improvements in quality, customer service and operational performance, delivering advantage right across the organisation. The Supplier has helped numerous public sector organisation realign their IT strategy with their business strategy to ensure IT is always optimised and fully aligned to business needs. The outputs of these reviews will be brought to you through the service review channels as appropriate, shaping your future plans and ensuring that services are effective in bringing business value to the Legal Ombudsman. We look forward to discussing this approach further with The Customer.

1.5 MANAGED INFRASTRUCTURE SERVICE

24/7/365 Environment Management

The Supplier will manage the The Customer infrastructure environment on a 24/7/365 basis in line with the agreed service level agreement. The Supplier's managed services division is comprised of 250+ staff across 3 principal practices: Applications, Database, and Cloud & Infrastructure managed services.

The Supplier provide cloud & infrastructure managed services to a broad range of customers in the UK and Ireland across a range of industry sectors: Public, Commercial, Financial, and Utilities. Our managed service customers currently include NHS Wales, HM Treasury, Irish Courts Service, Legal Ombudsman, Rural Payments Agency, 123.ie, Irish Continental Group, Local Government Management Agency, Brighton & Sussex University Hospital NHS Trust, Holiday Taxis Brighton, Goodbody Stockbrokers, NI Courts Services, and International Airline Group. More detail on the above engagements is set out in *Section 1.3.2.*

The Supplier's managed service delivery model conforms with ITIL best practice and is ISO20000 and ISO27001 accredited. At the core of our service is service desk which is fully staffed on a 24/7/365 basis. Our service desk engineering team will proactively monitor all The Customer's systems in the estate. Monitoring deployed on the estate will include network CPU, RAM storage, capacity, and service availability monitoring.

In the event of an alert or outage the service desk team will take immediate action. A ticket will

be logged on the LANdesk ITMS system, and if high priority, The Customer will be informed in-line with an agreed protocol. The service desk team will be responsible for managing the ticket from initiation to closure. If the incident cannot be resolved by 2nd line support, the service desk team will escalate to 3rd line expert specialist resolver groups for remediation. Following resolution of the incident, a full root cause analysis (RCA) report will be provided for high priority incidents, setting out in detail the reason for the outage and corrective action plan

In line with our service delivery model, The Customer will receive a monthly report setting out all incidents, problems, and changes implemented during the reporting period. The report will also set out how The Supplier has performed its managed service responsibilities against agreed service levels and KPIs over the quarter. This is covered in detail in our response to *Section 3.4.12.*

Azure Server Management

The Supplier's infrastructure managed service practice has a wide range of expertise and operational experience in monitoring and managing all types of servers and services across our teams, including Microsoft Azure. We have over 120 Microsoft certified staff. Certifications include: MCSE: Private Cloud, MCSE: Server Infrastructure 2012, MCSE: Messaging Exchange 2013, and MCSA: Office 365.

The Supplier, in partnership with Microsoft, has developed an Azure deployment Reference Architecture that ensures our hosting solutions adhere to Microsoft and industry best practices for security, resilience and performance. We have successfully deployed Azure solutions for a range of enterprise customers including Ordnance Survey UK, Balfour Beatty, Electricity Supply Board (ESB), Paddy Power, Musgrave and Wood Group.

Monitoring on all systems will be done via Opsview software where a dedicated 24/7 The Supplier team will monitor and action any alerts on all The Customer systems. The teams which will be managing The Customer servers have expertise and work daily on Azure environments, all types of Microsoft servers and OS, Active Directory/LDAP, Exchange, Skype, SCCM. The Supplier Infrastructure Managed Service teams work alongside the dedicated SQL database, SharePoint and CRM Managed Service teams. The Supplier has deep technical experience and consulting expertise across the Microsoft stack which The Customer will have access to on an ongoing basis during the lifetime of the managed service.

Infrastructure Management

The Supplier has extensive experience across our MSP practice for the setup and maintenance of e-mail systems, web proxies, DNS, different backup system, account management, software patching as per our protocols on software patching.

Our monitoring solution Opsview will monitor performance of all hardware devices ensuring CPU, Memory, Storage are at acceptable levels. The Supplier will complete an initial analysis of the The Customer storage environment to establish a baseline of current storage capacity and performance. This baseline includes IOPS for each system and will enable The Supplier to manage and predict storage requirements and performance needs for The Customer going forward. Information gathering will enable future performance tuning and storage allocation.

The Customer network and network devices will be monitored using Opsview which will provide alerting if there are any issues on the The Customer network or devices. Opsview will provide a history of issues or spikes in network traffic which will help The Supplier troubleshot any issues or bottlenecks on the network. The Suppliers network team will perform full network management and maintenance of the network. As per a review of the complete infrastructure all systems will be checked for high availability and reliability which in turn will be set up for monitoring to ensure The Customer achieve the required high availability and reliability set out in the contact. The Supplier will design solutions to provide high availability for all applications, for example web applications will be load balanced over multiple web servers or a SQL database will be clustered.

LAN/WAN/Wi-FI

The Supplier will manage the LAN, WAN, and Wi-Fi environment on behalf of The Customer including all in-scope infrastructure components. The Supplier provides network support services for a broad range of customers including PEAC Finance, Goodbody Stockbrokers, 123.ie, Institute of Banking, Holiday Taxis, and International Airline Group.

The Supplier 24*7 service desk will monitor the The Customer network environment on behalf of The Customer, and will log incidents when monitoring alerts are detected or an issue is reported by the customer The service desk will triage the incident and resolve at Level 2, or escalate to the Level 3 network engineering team.

The Supplier has a dedicated network engineering team comprised of certified engineers who will provide Level 3 support for all in-scope The Customer network components including switches, routers, firewalls, web proxies, load balancers, and wireless components. In the event an incident cannot be resolved by the Level 3 support team, the team will escalate to vendor support and manage the incident to resolution. Network, wireless and security products currently supported by the Supplier network team include Cisco, Juniper, Fortinet, Sophos, Checkpoint, Barracuda, Sonicwall, and Citrix Netscaler.

This team will manage the configuration of all network components in the environment. This will include switch and router configuration, and management of firewall and security components (e.g. NAT rules, ACLs, VPNs). The Supplier will also manage configuration of wireless controllers, SSIDs and access/identity services relating to these.

The Supplier will also manage all WAN connectivity on behalf of The Customer, including internet and MPLS services, and Express Route connectivity to Azure if required.

The Supplier recommends implementation of a centralised syslog server for archiving system logs relating to network components, and a centralised configuration management system for implementation and tracking of configuration changes.

Network Documentation

The Supplier will maintain a network diagram describing the The Customer LAN and WAN environment and all associated network components. This is a standard technical documentation requirement that will be a deliverable from the technical discovery phase of the managed service transition process. An *Example Customer Network Diagram* as implemented for another customer is included as *Appendix M.*

In compliance with ITIL best practice, The Supplier will maintain a Configuration Item diagram setting out all configuration items deployed in the The Customer estate. The Supplier will use the LANdesk CIDB (configuration item database) to record technical information relating to all network components in the The Customer estate, including software versions deployed. Software patches will be applied in-line with patch schedule to be agreed with The Customer. Critical security patches to network components will be always be applied on a priority basis.

1.5.1 Managed Builds for Software and Hardware

The Supplier will manage the Builds by utilising the below technologies:

- Software Microsoft Deployment Toolkit (MDT)
- System Centre Configuration Manager (SCCM).

Below is an example of a compliance report on a software update done via SCCM.

[REDACTED]

The Supplier will integrate MDT builds with SCCM in order to control the customisations. We will maintain multiple desktop images and will apply the below process to ensure that any hardware/software updates maintain consistency across the board in terms of the base image in use.

The Supplier will review the current configurations used by The Customer and will use this as the baseline build. Any changes to the software or hardware will need to go through a change management process with the following tasks included:

- The Supplier will review new requirements.
- The Supplier will verify that the new requirements do not conflict with an already implemented configuration.

If the Change is hardware related (e.g. a new hardware model) the following tasks will be implemented:

- The Supplier will review the new requirement
- Copy the Baseline build including the task sequence and rename it to “NEW Task sequence UAT”
- Identify new hardware model
- Verify if the model supports the Operating system being deployed by the task sequence
- Download the latest drivers package from the Manufacturer
- Import them to the deployment tool and create a new rule to install those drivers on the requested models
- Adjust any scripts that are used to configure bios or hardware configurations
- Deploy the new build to a test machine
- Verify installation and configuration
- Request UAT from the costumer
- If any issues arise during the UAT an investigation and fix plan will take place
- If no issues are encountered as part of UAT, a test deployment to the production environment will take place
- If no issues are encountered in production, the task sequence “NEW Task sequence UAT” will be renamed to “Task sequence V2.0” for release/deployment control.

If the change is application/software related (e.g. a new version or software update is required) the following tasks will be implemented as part of the change management/release & deployment process:

- The Supplier will review the new requirement
- Verify any dependencies of the Software
- If necessary The Supplier will update any dependent software
- Review of the Version/update to check:
    - If the new version of the software has reported issues
- Any reported conflicts with dependencies
- If the Version is confirmed as being free of bugs/issues The Supplier will create a new deployment package to deploy the application
- The Supplier will deploy the package and perform verification of the configuration and application functionality
- Request UAT from the costumer
- If any issues arise during UAT an investigation and fix plan will take place
- If no issues are encountered as part of UAT the application will be deployed in phases to specific machine groups
- Compliance reports will be run during all phases of this deployment.

Any new software/version update will now be deemed to be part of the baseline build. The following tasks will need to be implemented to guarantee that all machines are updated with the latest company baseline build:

- The Supplier will create a change for the task sequence update to the build
- Copy the Baseline build and Task sequence and rename it to “NEW Task sequence

UAT”
- Update or add the new application package to the task sequence/build
- Test deployment to a test machine
- Verify installation and configuration
- Request UAT from the costumer
- If any issues arise during UAT an investigation and fix plan will take place
- Test deployment on production environment
- If no issues are encountered as part of UAT, a test deployment to the production environment will take place
- If no issues are encountered in production, the task sequence “NEW Task sequence UAT” will be renamed to “Task sequence V3.0” for release/deployment control.

All of the above rules and process will be synchronised with The Customer’s Hardware and Software Lifecycle management rules.

1.5.2 Security and Connectivity

ISO27001

One of the key principles of the Supplier Infrastructure Managed Service is security compliance with ISO 27001, and ensuring that The Customer assets are protected.

As a provider of IT managed services to enterprise customers, The Supplier is acutely aware of the importance of robust IT security framework to The Customer’s business. The Supplier will leverage its knowledge and experience to tailor the security control framework to fully meet The Customer specific requirements.

The Supplier fully understands the requirement for third party review of the security control framework and will fully engage on this exercise. The Supplier’s own IT security control framework is subject to third party audit and The Supplier are very familiar with the process and rigour applied to the requirement. Furthermore, The Supplier regularly participates in external security audits commissioned by its customers.

The information security policy The Supplier apply as part of our Infrastructure Managed Service is designed to protect The Customer, its employees and customers from all information security threats, whether internal or external, deliberate or accidental. The policy covers physical security of premises and encompasses all forms of Information Security such as data stored on computers, transmitted across networks, printed or written on paper, stored on tapes and diskettes or spoken in conversation or over telephone. All vendors will be directly responsible for implementing the Policy, and for adherence by their staff.

The information security policy is characterised as the preservation of:

- Confidentiality - ensuring that information is accessible only to those authorised to have access
- Integrity - safeguarding the accuracy and completeness of information and processing methods
- Availability - ensuring that authorised users have access to information and associated assets when required
- Regulatory - ensuring that The Supplier meets its regulatory and legislative obligations.

In The Supplier, our information security policy enforcement is supported by the following documents, guidelines, procedures, and standards:

- Information Security Handbook
- Information Security Policy
- Human Resource Information Security Policy
- Asset Management Policy
- Access Control Policy
- Cryptographic Controls Policy
- Physical and Environmental Security Process
- Operations Security Policy
- Communications Security Policy
- Secure Transfer of Information Policy
- Secure Development Policy
- Secure Engineering Principles
- Information Security Compliance Policy.

These documents are available for adapting / adopting to the The Customer environment if required. An example of our Information Security Policy documentation is included as *Appendix F - V1 - Information Security Policy* (separate PDF document). Our *Integrated Management System Governance Process* manual is included as *Appendix K.*

Annual Penetration Test

The Supplier will conduct an annual penetration test on the The Customer estate using an independent supplier as specified. The Supplier has worked with specialist security consultancies such as Espion, RITS, Ward and Integrity 365 on such reviews for existing Managed Service customers. The Supplier will create a remediation plan and complete the required steps to mitigate any risks identified.

Recently PEAC Finance and Goodbody have had such reviews completed on The Supplier Infrastructure Managed Service solutions. The Supplier were available to assist and answer any queries prior to and during reviews. The Supplier also participated in the review of the reports in conjunction with the customer and 3rd party, and implemented remediation actions arising from the audit.

Network Hardening

The Supplier will implement perimeter firewall at all ingress/egress points between the The Customer network, MSP network, 3rd party network, and the public Internet. Traffic flow will be controlled by way of defined ACL and NAT rules in line with network design best practice. All VPN connections over the Internet will be protected using SSL or similar encryption technology. All routers and switches deployed will be security hardening in line with industry best practice.

Change & Security

The Supplier will be responsible for maintaining the security of the The Customer network, including all external connectivity to/from third party networks. All changes to the network environment will be subject to rigorous change control, whereby compliance with industry best practice in regard to network security will be one of the key assessment criteria on submission of change

request to the Change Approval Board.

The Supplier has collaborated with a number of specialist IT security consultancies on prior engagements, enhancing our own expertise and as a result can readily source specialist expertise in the event The Customer has a particular IT security requirement that needs to be addressed.

Client Remote Access

The Supplier will fully support the secure remote access solution deployed in the The Customer environment. Version supports a wide range of remote client access solutions across its managed service customer base. We understand that each of our customer's organisation maintain their own standards in terms of security and 3rd party access and auditability. We can work with The Customer on deploying the most appropriate remote access solution that meets our requirements but also in line with the The Customer standards.

The token-based authentication system currently deployed by The Customer is similar to other token based authentication systems supported by The Supplier. In addition, The Supplier has implemented multifactor authentication (MFA) solutions for other customers including Firmus Energy. Additional layers of content control can be achieved through the use of remote device management solutions such as Microsoft Intune, which The Supplier has implemented for customers such as PEAC Finance.

1.5.3 Managed Switches, Routers and Firewalls

The Supplier will manage the network environment on behalf of The Customer including all in-scope switches, routers, and firewall components. The Supplier provides network support services for a broad range of customers including PEAC Finance, Goodbody Stockbrokers, 123.ie, Institute of Banking, Holiday Taxis, and International Airline Group.

The Supplier has a dedicated network engineering team comprised of Cisco certified engineers who will provide Level 3 support for all in-scope The Customer network components including switches, routers, firewalls, web proxies, load balancers, and wireless components. In the event to an incident cannot be resolved by the level 3 support team, the team will escalate to vendor support and manage the incident to resolution. Network, wireless and security products currently supported by the Supplier network team include Cisco, Juniper, Fortinet, Sophos, Checkpoint, Barracuda, Sonicwall, and Citrix Netscaler.

The Supplier notes that The Customer has Cisco ASA 5510 firewalls deployed in its physical environment, and has extensive experience in supporting this this product. We note that Barracuda virtualised appliances are deployed in the Azure environment, and The Supplier has experience supporting this product.

The Supplier team will manage the configuration of all network components in the environment. This will include switch and router configuration, and management of firewall and security components (e.g. NAT rules, ACLs, VPNs). The Supplier will also manage all WAN connectivity on behalf of The Customer, including internet and MPLS services, and Express Route connectivity to Azure if required.

The Supplier recommends implementation of a centralised syslog server for archiving system logs relating to network components, and a centralised configuration management system for implementation and tracking of configuration changes.

1.5.4 Enterprise Management Tools

Configuration Management

The Supplier has extensive experience the deployment and support of configuration management tools such as Microsoft SCCM. We manage Desktop environments for firmus Energy using SCCM, and have deployed and support SCCM for customers including PEAC Finance and Goodbody Stockbrokers. SCCM also integrates with InTune which would provide a single platform and inventory for both Desktop and Mobile Device Management.

The Supplier will manage configuration through our ISO certified Service Asset and Configuration Management process. Configuration Items (CI's) are logged into our Service Management toolset and will be used to manage Incident, Problems and Changes.

Service Automation

Version has invested in the development of service automation and regards this as an essential component of its infrastructure managed service operating model going forward, particularly public cloud environments. The Supplier has developed scripts to automate deployment and configuration for a range of cloud customers including 123.ie, Aer Lingus, and AIB Bank. Automation tools deployed by The Supplier include:

- Terraform – Server Deployment
- Puppet – Server Configuration
- Ansible – Application Deployment

In the context of The Customer planned migration to a fully Azure hosted solution, we envisage we will utilise the above automation tools to streamline the deployment and configuration of server instances and workloads, and recurring tasks, within the cloud hosted environment.

Value Add

As part of our adoption of public cloud services, The Supplier has started to implement the DevOps operating model, using development and scripting expertise to automate deployment and management processes. The Supplier can provide significant benefit to The Customer in this regard as the DevOps model matures and is adopted by the organisation

Housekeeping

In addition to monitoring and logging of the The Customer environment, The Supplier will carry out our standard housekeeping and reporting practices on the systems that we use to support our customers.

Examples of these logging and monitoring procedures are

- Password requests for customer systems are reviewed to ensure relevant references and reasons for request are logged against them
- Incident Quality Control - Post Incident Reviews (PIP) are carried out weekly on a selected set of incidents. Associated event logs are reviewed
- Patching level requirements
- Access logs reviews
- Periodic event log reviews – Event logs will be stored locally or exported to a central

location.

The Supplier apply both a reactive and proactive approach to housekeeping.

Reactive

When The Supplier detects an alert on the monitoring tool for a threshold breach we will investigate the issue and look to resolve same. For example, an alert is raised highlighting a capacity issue on a disk. The Root Cause of the issue is that IIS logs are using available capacity. The Supplier will advise The Customer on the best course of action to take. Examples of the type of options to deal with the above example would be:

- Logs to be archived on a different disk
- Logs to be deleted
- Create a Request for Change (RFC) in order to expand the disk.

Proactive

The Supplier will audit and baseline the tasks that need to be done on devices periodically. We will automate housekeeping activities for a number of tasks. Examples would be:

- Automated Script created to clear log files and free up space on a scheduled basis
- Database maintenance tasks jobs to be created to run housekeeping tasks.

Where possible The Supplier will address manual housekeeping tasks as part of the patching maintenance window.

Housekeeping tasks will also be logged into the scheduled task database. The Supplier uses a task scheduling database which will list all the routine tasks that must be carried out. See screenshot below of some of the Goodbody Stockbrokers scheduled tasks that The Supplier carry out for their Infrastructure Managed Service Provision.

[REDACTED]

Scheduled tasks will result in the opening of an IPC outlining the task that needs to be done and which resolver team will be assigned the ticket. There are currently 1,008 scheduled tasks in the database that are meticulously carried out and signed off.

Each task in the scheduling database has a run book associated with it. The runbooks are documented/updated by level 3 engineers. See screenshot below of a sample runbook that the Service Desk use to carry out a SOX compliance report that a major pharmaceutical customer requires. (Parts of the runbook have been cut or obscured for security reasons.)

[REDACTED]

[REDACTED]

1.5.5 Resilience, Continuity, and Disaster Recovery

The Supplier will undertake a review of all The Customer infrastructure to access the level of high availability currently configured and work with The Customer to do a system classification of all systems. Once the review and system classification is complete The Supplier will recommend which components need to be redesigned to meet the required level of availability. Once the redesign of systems is agreed these will be deployed and tested to remove the single points of failures to ensure The Customer receive the required

level of availability. The Supplier completes this exercise with all managed service customers as part of a transition into managed services.

The Supplier will look at each The Customer service as a whole and ensure each component is highly available, such as ensuring the web front end of applications is load balanced across multiple web servers. Databases will be clustered to ensure high availability of the database component. The Supplier will also look at all other components which across the The Customer infrastructure estate to ensure if there is a single failure the complete service maintains availability.

The Supplier's own business continuity process is included in the scope of our ISO 20000 & ISO 27001 certification and is audited periodically by the internal and external auditors.

Support Service Business Continuity

We have invested heavily to remove any single points of failure from our critical services infrastructure. LanDesk, our service management application and SharePoint, our run book and knowledge base repository are running on an "always on" highly available SQL Server stretch cluster. Data on the primary database is replicated in real time to an onsite database and to a database running in the cloud. In the event of a single failure causing one of the onsite servers to go offline, the second onsite server can quickly be switched over to become the primary server. In the event of a failure that causes both onsite servers to go offline, the cloud instance can be scaled up to handle the required volume and be promoted to the primary server. The Supplier's DNS is managed though Amazon Web Services, so changes are not dependent on the onsite infrastructure. Our DNS records are configured with a very low time to live, so changes are propagated very rapidly.

All monitoring and infrastructure support systems used by Opsview, The Supplier's monitoring tool, including network hardware, servers, and Internet connectivity are redundant between our monitoring servers. The Opsview service is supported by a:

- Primary master
- Secondary master, providing high availability
- Failover master, providing a disaster recovery platform, this server is housed in our secondary datacentre

In the event of a master failure the monitoring slave will detect the failure and proactively re-establish the service on the secondary master or disaster recovery server. Failover tests on all of these services are carried out annually. The output from the tests is included in the scope of The Supplier's quarterly ISO 20000 audits. Our business continuity plan is invoked if one of the main The Supplier offices becomes unusable.

The Supplier's business continuity team carry out six monthly table top exercises to improve our understanding of the business risks. These workshops involve analysing the potential impact of different failure scenarios and developing a plan to address those scenarios. Topics covered to date include:

- Failure of one HQ building
- Failure of both HQ buildings
- Failure of the primary Internet connection
- Failure of the Opsview master
- Failure of one of the datacentres.

The introduction of a stretched "always on" cluster with a cloud component was an action for the table top exercise reviewing the impact of both main The Supplier buildings.

Our business continuity plan has been designed to ensure that service issues are not noticed by our customers. We are willing to share our business continuity plan with The Customer and to plan joint exercises. We can also work with The Customer to provide ICT disaster

recovery advice and carry out periodic testing of The Customer disaster recovery processes, as a service we provide to a number of our larger customers.

In addition to our own business continuity arrangements as detailed above, The Supplier will provide and manage the disaster recovery services in Azure and the MS Online configuration and ensure these disaster recovery services are fit for purpose to deliver the require standard for The Customer. The Supplier will provide and manage disaster recovery services to the wider IT infrastructure. The Supplier will plan, detail documentation, complete the DR failover test, record the results, update the documentation of any changes and complete any remediation of the process or infrastructure after the tests. This process will be completed on annual basis. An *Example DR Plan* is included as *Appendix H*. An *Example DR Test Report* is included as *Appendix I.*

1.6 CONTINUOUS IMPROVEMENT

As part of our The Supplier Infrastructure Managed service, The Supplier look to provide continuous improvement in all areas that we provide support. The Supplier commit to **Continual Service Improvement** and will work with The Customer to develop an IT roadmap. The Supplier can add most value to The Customer through a continuous service improvement process and a transformation programme in the form of technology improvements, upgrading and replacement of legacy systems, or process, user experience and performance improvements. All in line with the enterprise architecture principles we will maintain for your services.

Through our partner network and accreditations**,** we have direct access to vendors' expertise and assets. We evaluate new technologies and determine if they will bring competitive benefit to our customers and access to our most highly skilled resources enables our customers to innovate and plan continuous improvement. For example, The Supplier an accredited Amazon Web Services Partner and we are a Microsoft Gold partner in 12 Competencies. Accordingly, The Supplier is uniquely positioned to advise The Customer on the opportunity and potential of cloud services.

Our proven experience and quality of our customer references will demonstrate our ability to work with The Customer to develop a roadmap to modernise, streamline, and strengthen the infrastructure and associated services, some examples include:

[REDACTED]

[REDACTED]

For evaluation purposes, please see our response to *Section 3.4.14* for further information regarding The Supplier's approach to CSIP.

1.7 MANAGING CHANGE
1.8

The Supplier operates a comprehensive change management process where the purpose is to control the lifecycle of all changes. The objectives of change management are to:

- Respond to the customers changing business requirements
- Respond to business requests for change
- Ensure changes are recorded and evaluated
- Ensure that authorised changes are prioritised, planned, tested, implemented, documented and reviewed in a controlled manner
- Ensure that all changes to configuration items are recorded in the configuration management system
- Minimise risk where possible otherwise accept and monitor

There are four different types of changes within the change management process. These are:

- **Standard Change** – A pre-authorised change that is low risk, relatively common and follows a documented procedure (runbook) or instructions. In order for a change type to be considered a standard change it must be pre-approved by the customer.
- **Emergency Change** – A change that must be implemented as soon as possible, for example to resolve a major issue or prevent one from occurring (see Section 2.4.15.1)
- **Normal Change** – Any change that is not considered a standard change or emergency change
- **Major Change** - Changes that have the potential to have a major impact on a service, although still logged as change requests, such changes will be handled via the Design and Transition of New or Changed Services process (Transition Management)

For changes not contained in your standard change catalogue the Change Initiator will create a Request for Change (RFC). An RFC template will be agreed during transition and would typically require the following information:

- **Trigger** - Relating Incident or Problem record, Business need, Purchase Order
- **Description** – Both business level and technical
- **Business Case/Reason** – Full justification
- Effect of Not Implementing
- **Configuration Items** – Details of CIs and if any changes to the CMDB are required
- **Contact Details** – For change initiator and person proposing change
- Date and time of proposal
- **Change Impact** – Minor, Moderate or Major
- **Predicted timeframe** – time required to implement change and proposed implementation time.
- **Back Out Plan** – remediation steps should change fail
- **Cost** – cost of implementing the change (and any hyper-care provision)
- **Authorisation Date and Signature** (Inc. electronic)

This information will be added to the Change Register which will facilitate in-depth analysis of change patterns, work-loads and dependencies and therefore will contribute to change management decisions (e.g. time/cost/business impact projections).

The following is a sample RFC Template:

[REDACTED]

[REDACTED]

A RFC will require input from different sources and the Change Initiator (Requester) should coordinate this task if they are in a position to do so, otherwise a suitable representative from either The Supplier or The Customer will own this process to ensure the proper formulation of the request. Once all information has been added to the RFC, the RFC will be attached to

the Change Record and passed to the customer for approval by the appropriate The Customer Change Authority.

We included a process view of our Change Management Process in the response to *Section 3.7.5.*

1.7.1 Expertise & Third-Party Relationship Management

The Supplier is a Microsoft Gold Partner with strong and demonstrable expertise in Office 365 and Azure services. We have been working in the Microsoft technology arena since 2006 and today we are recognised as one of the most competent partners in the UK and Ireland. We bring a breadth and depth of expertise across the Microsoft stack allowing us to look beyond specific requirements to underlying customer issues and to deliver integrated technology solutions that leverage the entire technology stack in the cloud.

As can be seen by our partner certification, The Supplier has a total of 14 competencies including Cloud Platform (Azure), Cloud Productivity (O365), CRM (Dynamics), Collaboration & Content (SharePoint), Datacenter, Devices and Deployment, all of which have a direct relevance to the The Customer Infrastructure requirements.

In addition, and of particular relevance to The Customer and our proposed infrastructure solution hosted on Azure, The Supplier has recently been accepted into the Microsoft Azure Engineering Program for Partners. The Global Program has only been opened up to 10 Microsoft Partners around the world (The Supplier is one of only two partners selected from Western Europe) and is based on evidence of significant customer projects successfully delivered in Azure.

The Program is being run by the Azure OS Development Engineering team in Microsoft and will cover Azure Compute and Storage. The Supplier has bi- weekly calls with the Azure Engineering team providing us with a "Direct Line" into the engineering team developing Compute and Storage offerings for Azure.

The Supplier were selected due to our breath of technical expertise across both Microsoft (CRM, SharePoint, O365), and other cloud platforms including AWS. The deliverable from the program is to facilitate feedback from Partners directly to Microsoft engineering from the front line of Azure project delivery.

Further to the provision of Cloud services via Microsoft, Oracle and AWS, The Supplier also provides a UK Government certified private cloud capability where we are hosting systems at Official & Official Sensitive level for organisations such as HM Treasury, Great Manchester Police, and Cambridge University Hospitals NHS Foundation Trust.

To deliver this contract, The Supplier do not require the skills of any subcontractors or 3rd parties, with all services being delivered by the combined The Supplier team. This means that there will be no commercial, cultural or contractual tension with our team and all the team will be pulling together to deliver an excellent service to The Customer.

The Supplier will act as a single point of contact for all ICT issues logged with the Service Desk. This includes logging and managing issues on third party supplier systems and equipment.

We do however recognise that there will be times when we need to engage with, and work alongside, other 3rd party suppliers during the lifetime of the contract. All of the current The Supplier support and development contracts involve on-going liaison with our customers' staff and in many

cases other third party providers.

Our approach here is to take ownership of issues until conclusion and we recognise that liaising with third parties is key to the successful delivery of an excellent Managed Service. We have a *"customer first"* attitude and take responsibility for any issue. We not only build our relationship with you, we also build a relationship with your other suppliers to deliver an optimum service.

An example of this is where we may need to engage with Microsoft about issues or incidents relating to the hosted solution or underlying infrastructure. Using our ISO certified processes we have experience of managing the Microsoft relationship on behalf of our customers. Indeed, we currently carry out this role already for The Customer through our existing CMS Managed Service and demonstrated this strong relationship to good effect during the recent CRM Upgrade Project during the summer of 2016. This role involves various operational activities including managing:

- the scope & objectives of work tasks
- allocation of work and coordinate activities between vendors
- performance against expectation
- managing major incidents regardless of sources (service provider)

In terms of looking at future enhancements to the The Customer solution we have the skills and expertise to be an effective partner over the longer term. Under our Microsoft Capability we have dedicated teams specialising in Azure, System Centre, Networking, Office 365, Dynamics CRM, and SharePoint. The capability has over 150 dedicated consultants who are Microsoft certified across the various competencies.

As a certified Microsoft Cloud Service Provider (CSP), The Supplier has engaged directly with Microsoft in response to the The Customer ITT. The Ministry of Justice (MoJ), and associated agencies, are classed as a "Hypo Account" within Microsoft, meaning The Supplier can access a dedicated team to support activities relating to technical, solution design, implementation, commercial modelling, etc. We will continue to realise the benefits of being a certified CSP to ensure effective support and operation of the The Customer infrastructure solution throughout the duration of the contract.

1.7.2 Change/Project Governance & Process

We envisage the The Customer cloud transformation project (and any project during the lifecycle of the contract) will be delivered using the 1-Manage project management methodology which is based upon PRINCE2. There are a number of key principles which we will adhere to in managing the The Customer project:

- Project should have continued business justification throughout the lifespan of the project regardless of changes made - sufficient business benefit must continually exist for the project to continue
- The project should seek to learn from the experience of others in the organisation and other projects, and must ensure that lessons are captured for future use
- Project should define roles and responsibilities, so that all working on the project are clear what is expected from them, and so that all stakeholder's interests are sufficiently represented
- Project should be managed in stages, the number of which will depend on the project type and duration and the control requirements of the Project Board
- Project should be managed by exception, meaning agreed tolerances should be defined for key project objectives (time, cost, scope, quality, risk and benefits), the Project Management Team then work within these tolerances and report exceptions to the next level of authority where tolerances are likely to be exceeded
- Focus on products, when planning, delegating, monitoring and controlling the project.

The Supplier methodology has defined processes around:

- Quality Management
- Planning
- Risk, Issue and Change Management
- Monitoring and controlling progress.

In addition, our methodology specifies the set of activities required to manage each stage of the project lifecycle. All of these processes are supported by a comprehensive set of documents, which help to ensure that nothing is overlooked and everything is controlled in a correct and timely fashion.

Project Structure & Governance

To ensure that all projects (large of small) during the lifetime of the contract are delivered on time, budget, and to agreed quality standards, we envisage the following governance structure is put in place from the initiation stage:

Project Team: The project will be delivered by a project team consisting of core members from each technical area. There will also be an extended project team that will comprise resources from area's that are temporarily assigned to the project for specific activities.

Project Board: A project board will be established to oversee the overall project delivery and governance. The board will consist of management functions from relevant parties that have significant involvement in the project delivery.

Change Control Board (CCB): A change control board will be established to review and impact assess all requests for change (RFC). The CCB will have authority to approve RFC's to a defined tolerance level (will be agreed during project initiation). If the RFC exceeds the CCB tolerance it will be submitted to the project board for review and approval. The Change Control Board will be established to review and The RFC will be reviewed by the project team (or a subset of)

Communication Plan

Weekly Status Report: The project manager responsible for delivery of the The Customer project will distribute a weekly project status report outlining the project progress.

Weekly Project Meeting: A progress review meeting will be held once a week between all project team members. All open actions, issues & risks will be reviewed at the weekly meeting. New change requests will be reviewed and approved if they are within project team approval tolerances. The project manager will circulate an agenda in advance of the meeting and circulate the meeting minutes after the meeting

Monthly Project Board Meeting: A project board meeting will be held monthly from the Commencement Date. The project board will review the overall status of the project including schedule, scope and budget. It will also approve project changes and exceptions that are above the project team tolerances. The project manager will circulate an agenda in advance of the meeting and circulate the meeting minutes after the meeting.

Other Meetings: Meetings will be scheduled as required during the project duration. These meeting will include design meetings, document review meetings, test planning meetings.

Documentation Management

A SharePoint Online External Collaboration site will be created for the The Customer project. The site will contain the project artefacts. The project team will have access to the collaboration site. All project documents that require approval will be version controlled.

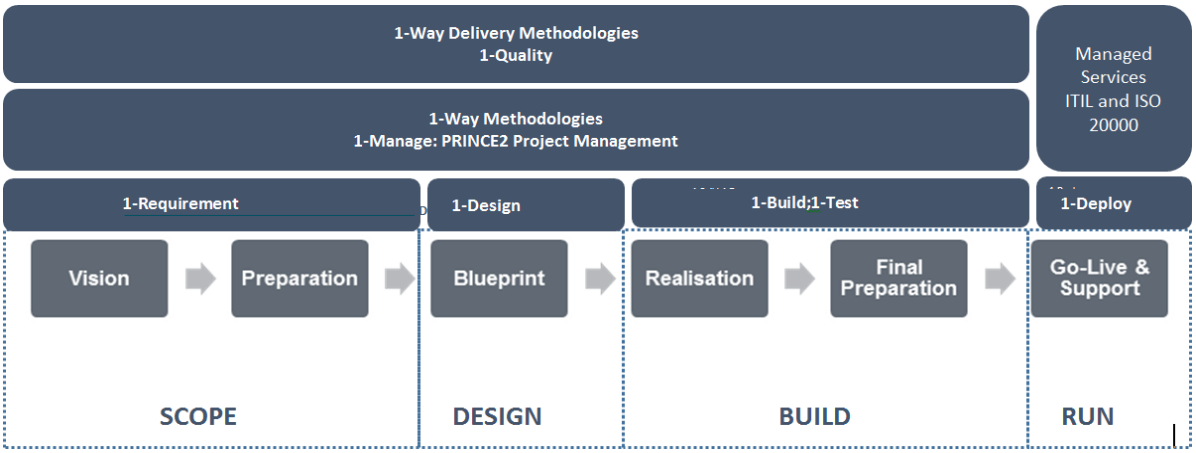
Quality Plan

A quality plan will be drafted to outline how quality will be achieved during the project. The plan

will document the required test plans, logs and checklists to verify the project quality. A traceability matrix will be used to track the requirements to operational processes and acceptance testing. All project risks and issues will be tracked in the RAID log.

Change Control

The change control process will manage changes to any in flight projects, schedule and budget. If a change is required a Request for Change (RFC) will be drafted. The project manager will log the change request in the Change Register and schedule it for review by the Change Control Board (CCB). The CCB will review and impact assess the request against the scope, schedule and budget. If the request is within the CCB defined tolerance level then they can approve the request. If the RFC exceeds the CCB tolerance it will be submitted to the project board for review and approval.



Delivery Methodology

We also maintain a “Forward Schedule of Change” which outlines all planned changes and which is reviewed by our Change Advisory Board (CAB) on a weekly basis. This will include any upgrades to Microsoft Online services and associated add-in’s to ensure that any affected services remain no more than 1 version behind the latest available. We will also proactively maintain any firmware and software relating to the infrastructure ensuring all related items are maintained and kept as up to date as possible.

Execution plans as well as backout plans are scrutinised to ensure that risks have been properly assessed, plans tested where possible, and that stakeholders have been appropriately notified. In the case of systems which we monitor or where we provide support outside normal business hours, this may also include switching off alerts for a short period and notifying on-call personnel of the work to be performed. Additional senior technical input and QA will be sought if deemed necessary.

Of course we recognise that from time to time changes may be needed at short notice to address the unforeseen. Regardless of the emergency situation we ensure that similar scrutiny is applied to all Emergency Changes to ensure that the core principles of change management are adhered to so as not to exasperate the situation which the change is intended to address.

You will have full access to our Request for Change Forms via LANDesk. We are also happy to provide extracts from the Forward Schedule of Change for all The Customer entries.

We have included for reference and evaluation purposes a full copy of our Change Management Process as *Appendix C - MSP Change Management Process* (separate PDF document attached to submission).

Change Advisory Board (CAB)

All infrastructure changes must be approved by the Change Advisory Board (CAB). Any change to a production environment must be logged to the Forward Schedule of Change. An Emergency CAB can be called in an emergency situation. The Supplier's CAB meets on a weekly basis.

The CAB will make use of the following items in order to consider the **impact** of the change and /or released proposed upon the business.

- The details provided in the **Forward Schedule of Change** (FSC) log.
- The Configuration Item Diagram (CID).
- The list of Configuration Items (CIs) affected by the change. (from FSC log)
- **Request for Change** documents.
- Release Plan
- Level of testing carried out to date
- Rollback procedures
- The relevant consultant(s).
- Any other relevant information

It should be clear from the above that due consideration has been taken to ensure changes are implement in a controlled and measured manner. This ensures business readiness for the proposed change and the readiness of those who will be involved in provided the technical support.

If satisfied with the release plan and the necessary resources are in place to implement the plan as scheduled, the CAB will approve the production release.

If the CAB is not satisfied the release will be rejected and the release plan must be addressed where weak and re-submitted to the CAB.

Any changes that are wholly or partly unsuccessful will be reviewed at the following week's CAB and a root cause analysis and lessons learned document may be requested, depending on severity of any issues encountered. This ensures we avoid repeat failures and that our processes continuously improve.

1.7.3 Requirements & Options

The Supplier's mission with all of our Managed Services customers is to deliver business benefit through technology. Our staff are hired, trained and challenged to understand complex business challenges and issues and find effective solutions to these and understand how these can be implemented. The Supplier has a culture of a challenger mentality, and this mentality coupled with our public sector focus and experience allows us to work in partnership with our customers over the longer term to provide business improvements.

The Supplier will work closely with The Customer on the requirements and options for change

on the infrastructure estate and associated systems/services. We fully understand the risks regarding implementing tactical changes or strategic projects while at the same time providing critical business support to the core The Customer infrastructure.

We address this issue very early in our evolution by establishing two distinct lines of business – our support (Managed Services) and projects (Business Solutions) practices. We know from experience the only way to achieve success in both project delivery (small or large) and business support is dedicating teams to their respective objectives.

The support and project practices have distinct processes and aims. Managed Services has implemented ITIL aligned best practice IT service management. Typically managed services are involved in long term support engagements (which may include some tactical change). Business Solutions adhere to the project management methodologies of the "1-way" and Prince 2. We have explained in detail throughout this response how these are managed within The Supplier – see *Section 3.* for reference.

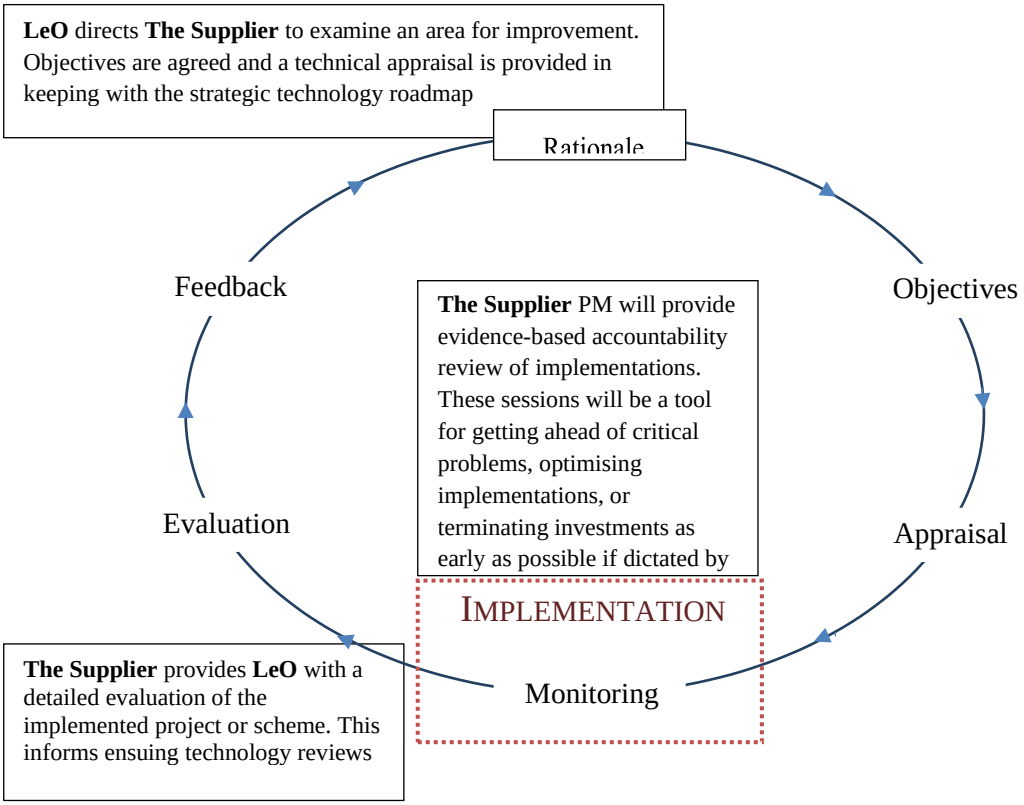
The Supplier will continue to work in partnership with The Customer on the in- place technology and make it better. We have unparalleled expertise at our disposal in this regard across the organisation, and we also have an excellent understanding of the Legal Ombudsman through our existing relationship under the CMS Managed Service. This gives us a unique opportunity to support The Customer in the short and long term to improve not only the technology elements of the organisation, but also the business and operational areas where we can identify refinements or enhancements that will deliver business value.

Through the Supplier capability structure where we have teams and technical streams focusing on specific technologies, skills and approaches, we can garner ideas, initiatives, and innovations that we can present to The Customer for consideration for business improvement. We have an Advisory Services Team whose role it is to work across the capabilities, and our customer facing teams, and surface these ideas and bring them to our customers in a way that is relevant to their business and operational challenges. The Customer will benefit from this approach and capability structure as we bring new requirements and options across the following areas:

- Business Transformation, Enterprise Architecture and Change
- Microsoft Solutions
- Oracle Solutions
- Amazon Web Services (AWS)
- Application Development & Management
- Data Management & Business Intelligence
- IT Service Management & Managed Services (24/7 ITIL, ISO 20000, ISO 27001 certified)
- Cloud Integration
- Digital Transformation
- Software Licence Management

We will use best practice approaches to analyse any proposed changes, high level requirements, tactical or strategic objectives, and assess their potential benefits and outcomes This guidance will help initiate projects, capturing the measurable benefits and/or costs to The Customer as part of the appraisal in the process. Once changes have been delivered a retrospective analysis

at completion, conclusion or revision will be conducted and fed back into the process.



The Customer's ability to bring new legislation, policies, strategies, projects and requirements will only achieve their objectives and deliver benefits if they have been scoped and planned realistically and robustly from the outset and the associated risks taken into account. The Supplier will leverage its domain expertise and technical capability to inform, challenge and suggest solutions which fit the needs for each individual requirement whilst also considering the potential wider impact on the overall The Customer solution.

This will allow for the production of a business case for the potential system requirement. The business case, both as a product and a process, provides The Customer decision makers and other stakeholders with a management tool for evidence based and transparent decision making and a framework for the delivery, management and performance monitoring of the resultant scheme.

Where the scope of the underlying objective is non-contentious and can be fulfilled by existing The Customer / The Supplier resources, a one stage business justification case will be provided to The Customer business owners.

Where a more thorough appraisal is required, The Supplier will provide a strategic outline programme in support of a new policy, strategy, transformation programme. This partnership approach will allow The Supplier to bring its experience to bear, countering and challenging The Customer's ideas and preferences where necessary and appropriate, in order to deliver the most effective outcome for any change or proposed enhancement.

The strategic outline programme will evidence:

- The “**strategic case**” – That the intervention is supported by a compelling case for change that provides holistic fit between the The Customer and other associated stakeholders;
- The “**economic case**” – That the intervention represents best public value;
- The “**commercial case**” – That the proposed intervention can be procured and is commercially viable;
- The “**financial case**” – That the proposal is affordable;
- The “**management case**” – That what is required from all parties is achievable.

It is in this final regard that the Supplier dedicated project manager and business analyst will be particularly effective. As The Customer processes manifest across multiple stakeholders and various system components acting in unison, The Supplier will provide the necessary attention to these matters to guarantee business objectives are achieved. These activities will also guarantee that very significant changes can be brought about without any detrimental impact on the day-to-day operational and business activities of The Customer and the core technology infrastructure.

Whilst any strategic programme undertaken by The Customer will consider the above in order to achieve approval and provide the platform for ongoing project activities, The Supplier will also ensure that we will take into account the The Customer IT governance principles at all stages when considering and proposing potential solutions:

- Decided by Strategy
- Decided for the Organisation
- Decided by Business Case
- Designed to Serve Customers
- Designed for Usability
- Designed for Efficiency
- Designed for Longevity
- Designed for Interoperability
- Designed to Comply
- Delivered with the Business
- Delivered using Good Practice
- Designed for Continuity.

1.7.4 Testing & Assurance

The Supplier’s Quality Management and Testing approach is something that is planned in from the outset, not inspected at the end of a project or change and therefore must be embedded throughout the lifecycle of the change or project.

The level of testing that may be required (or warranted) will be determined by the type of change being implemented. For a large change our Test Planning will detail the following

- Definition of Test Phases (& definition of Test Bed)
- Scope of Testing to be undertaken within each Test Phase
- Test Lifecycle and Execution Procedures

- Test Inputs & Outputs for each test Phase
- Data Pre-Requisites & Data Issues
- Bug Raising, Resolution & Management

We employ our best-practice methodology 1-Test, which incorporates a modular test methodology which provides for the creation of test conditions from the very beginning of the development (or patching) lifecycle. Tests are created once and executed many times across the project lifecycle.

In this way we can assure that any changes or enhancements to the platform, patch-levels, interfaces etc. will be fit-for-purpose and performant when transitioned into production.

We believe that UAT activities are the final crucial gateway prior to production. As such, we will ensure that your users are fully supported throughout this phase to ensure that queries are handled and issues are logged and addressed. The Supplier manage and track all bugs through Bugzilla.

We also realise the importance of not assuming that business users have the necessary experience or skillsets to effectively test changes to line-of- business systems from a UAT perspective. Therefore, as part of the change review process we will work with you to determine the complexity of UAT and what level of support may be required. Such support may include any or all of UAT management, generation of scripts, updating of business documentation / process documentation etc.

We note The Customer's desire to undertake its own changes wherever it has the capability and capacity to do so. In this scenario, The Supplier would recommend that The Customer only undertake less complex or less significant change items, and following a defined and agreed process as outlined below.

The Supplier can assist The Customer staff in knowledge and skills transfer during the course of the managed service contract in order to support The Customer in making its own changes. We understand that this is an area of particular importance to you given the drive toward self-sufficiency in the public sector.

We have established a formal skills/knowledge transfer approach which we have been successfully utilising with a number of our clients in the public sector. Our skills/knowledge transfer approach has meant that our clients have been able to efficiently up-skill their own internal resources and build internal expertise in certain areas. We would be pleased to consider this for the The Customer staff and welcome further discussion in this area.

In regards to The Customer wishing to undertake its own changes we do not see this as an area of concern on the basis that the procedures in place by both The Customer and The Supplier are very closely mapped with our adoption of the ISO 20000 standards.

All changes should adhere to the change management process implemented as part of the support agreement and outlined in *Section 3.7.5.*

1.7.5 Environments & Deployment

Change is the one constant in the provision of an IT service. LEO will be implementing change to your IT environment and understand that change carries risk. A large percentage of all IT

failures are directly related to poorly planned or poorly implemented change. Therefore, LEO require strong change and release management processes to be put in place to ensure all changes are appropriately planned and implemented.

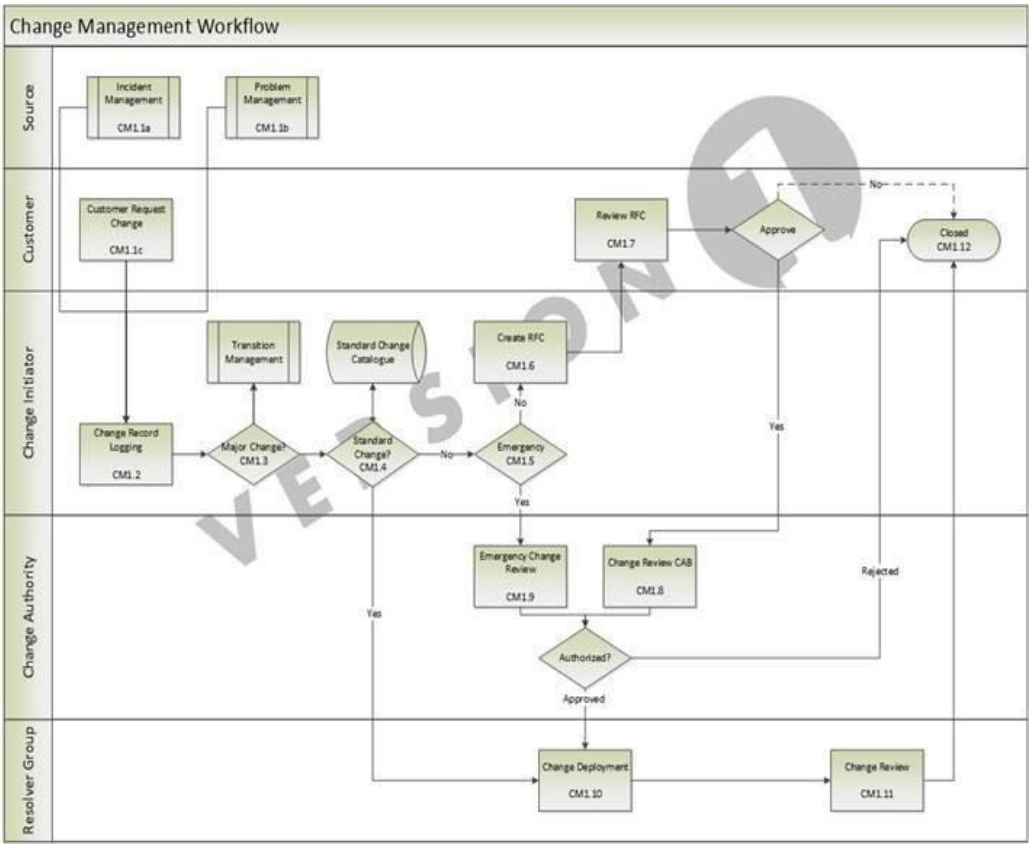
The Supplier operate a mature and comprehensive change and release management policy and processes. The policy and process is ingrained within all of our Managed Services operations. The process is subject to internal and external audit and has been validated to ISO20000 standard since May 2011.

Before any change is installed, a full backup of all data and server configuration information must be made. The Supplier will apply best practices for disaster recovery and will incorporate periodic testing of the restore process to ensure the integrity of the backed up data.

As part of the Supplier change management process a working backup is a prerequisite for any Request for Change (RFC) to be approved on the change advisory board (CAB).

Change management is vital to every stage of the process. Any environmental changes must have associated contingency and back-out plans should something go wrong during or as a result. Information on risk mitigation will be included in the release management notes. Monitoring and acceptance will also be included in the change management process.

Out Service Desk tool LANDesk is workflow based and fully compliant with our ISO20000 certified process.



CM1.1 Initiate Change

A change can be initiated by the customer or as an output from the Incident and Problem processes. A change initiator will be appointed to each change. It is their responsibility to record the change request and log all the available information

CM1.2 Change Record Logging

Once a request is received for a change a Change record is logged. The level of detail recorded depends on the size and impact of the change. Information will be added to the change record as it progresses through the lifecycle. The change record will hold the full history of the change, where applicable this will include RFC, authorisation, implementation and review information

CM1.3 Major Change

Changes that have the potential to have a major impact on a service, although still logged as change requests, will be handled via the Design and Transition of New or Changed Services process (Transition Management).

CM1.4 Standard Change

A check is performed to see if the change type is contained in the Standard Change Catalogue. The Standard Change Catalogue is a list of pre-approved minor changes that have been approved by the customer and have documented instructions. If the change type is contained in Standard Change Catalogue the change will not require an RFC or CAB approval. Standard changes will be implemented without CAB approval, however they will be reviewed after implementation under the change review process

CM1.5 Emergency

The Change Initiator must determine if the change is to be classified as an Emergency Change. This is done by determining if the change is required to fix an ongoing issue or to prevent one from occurring. If the change is classified as an emergency the Change Authority must be notified and an Emergency Change Approval Board will be convened to review the change.

A RFC and customer approval is required for Emergency Changes, however to ensure the implementation of the change is not delayed, these can be done in parallel with the Change Review i.e. the change can be reviewed and approved on the basis that customer approvals is received prior to implementation.

CM1.6 Create RFC

For changes not contained in the standard change catalogue the Change Initiator will create an RFC. A The Supplier RFC template is used and will require the following information:

- Trigger - Relating Incident or Problem record, Business need, Purchase Order
- Description – Both business level and technical
- Business Case/Reason – Full justification
- Effect of Not Implementing
- Configuration Items – Details of Cis and if any CI changes are required
- Contact Details – For change initiator and person proposing change
- Data and time of proposal
- Change Impact – Minor, Moderate or Major
- Predicted timeframe – time required to implement change and proposed implementation time.
- Back Out Plan – remediation steps should change fail
- Authorisation Date and Signature (Inc. electronic)

A RFC will require input from different sources, the change initiator will coordinator this task. Once all information has been added to the RFC, the RFC will be attached to the Change Record and passed to the customer for approval

CM1.7 RFC Review

All RFCs will be reviewed by the customer impacted. This review is to ensure that all information has been provided and the requirements and goals are accurate. The affected customer will be required to approve the RFC before it can be presented to CAB for authorisation.

CM1.8 Change Review

CAB meetings will take place weekly and all available CAB members are required to attend. During these meetings all customer approved normal changes will be reviewed. Change Initiators will be required to attend and present their change. CAB members will ask questions on each change and evaluate before authorising.

To prevent unnecessary delays, changes with minor impact can be reviewed outside of the weekly meeting. This is done by contacting the Change Authority via email a minimum of 24 hours before the target change implementation time. The Change Authority will first confirm the Change is correctly set as minor impact before proceeding with a full review. If necessary the Change Authority may decide that a normal change with minor impact is best reviewed at the weekly CAB meeting, the change Initiator will be informed of this decision.

CM1.9 Emergency Change Review

A subset of CAB members with specific expertise and responsibility will be convened to review emergency changes. This group are known as the Emergency Change Advisory Board and will review and evaluate changes outside of CAB meetings. All CAB members will be informed of raised emergency changes before they are authorised by ECAB.

CM1.10 Change Deployment

Once a change has been authorised it can be deployed at the approved time. Deployment of changes that are part of release will be managed as part of the release management process. All other changes will be coordinate by the change management process. Change management has the responsibility to ensure that changes are deployed as scheduled. Changes that are subject to multiple deployment stages will require RFCs for each deployment and individual change authorisation.

CM1.11 Change Review

After a change has been deployed it will be reviewed to determine its success. The aim of this review is to confirm that there is no adverse performance impact, no unacceptable risk and the goals of the change have been achieved. If this review shows the change is acceptable then it will be set to successful. If the review shows the change to be unacceptable it will be set to failed. All changes will be forwarded to customer for final review and closure.

CM1.12 Change Closure

Before a change can be closed it must be reviewed by the customer. The customer will assess the findings of the change review. If the change has been successful it will be closed without further action. Where a change has failed to meet its objectives further actions may be required. These actions will be handle in a new Change record.

Network:

	Management
1	Log files management
2	Scheduled tasks
3	Log/Event log files monitoring
	Monitoring
1	Standard performance monitoring template
2	Customer template for monitoring
3	Device and port availability
4	Port errors
5	VPN status
6	Bandwidth utilisation
7	Capacity management and monitoring
	Error Handling
1	Incident management

2	Problem management
3	Service level agreement

Key Activities	
1	Managed Services Status Reports - Monthly
2	Managed Services Status Reports - Quarterly
3	ITIL process management (incident, change, problem, etc.)
4	Monitoring & Alerting
5	Service Desk
6	Service Delivery Management

Out of Scope	
1	Asset management
2	New network devices implementation
3	Cisco/Citrix OS upgrades

Assumptions	
1	Firmware patching only if required by vendor support
2	

Database:

	Management
1	Log file management
2	Scheduled tasks
3	Log/Event log files monitoring
4	Extra, local backups management
5	Database maintenance

	Monitoring
1	Standard performance monitoring template
2	Customer template for monitoring
3	Database monitoring template

	Error Handling
1	Incident management
2	Problem management
3	Service level agreement

Key Activities

1	Proactive Daily/Monthly Checks of Databases
2	Annual Database Health Checks
3	Managed Services Status Reports - Monthly
4	Managed Services Status Reports - Quarterly
5	ITIL process management (incident, change, problem, etc.)
6	Monitoring & Alerting
7	Service Desk
8	Service Delivery Management
9	24x7 Service and on-call out of hours 2nd and 3rd level support for in-scope systems.

	Out of Scope
1	Asset management
2	New software deployment
3	Patching databases
4	Database version upgrades
5	Database deployment and commissioning

Infrastructure:

1	Log file management
2	Event log management
3	Log/Event log files monitoring
4	Scheduled tasks
5	Escalation of issues to third parties
	Monitoring
1	Server availability
2	Standard performance monitoring template
3	Customer template for monitoring
4	Key Services Monitored - details
5	Storage capacity monitoring
6	Alerting
	Security
1	Hardening applied
2	User management
	Error Handling
1	Incident management

2	Problem management
3	Request Management
4	Service level agreement

Key Activities	
1	Managed Services Status Reports - Monthly
3	ITIL process management (Request, incident, change, problem, etc.)
4	Monitoring & Alerting
5	Service Desk
6	Service Delivery Management
7	24x7 Service and on-call out of hours 2nd and 3rd level support for in-scope systems.

Out of Scope	
1	New software deployment - RFC Process
2	Major Version Updates - Service Pack Deployment - RFC Process
3	Server deployment and commissioning - RFC Process

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:

1. DEFINITIONS

1.1 The following terms used in this Call Off Schedule shall have the following meaning:

"Maximum Percentage Mark Up Rates"	means the maximum percentage mark up the Supplier may add to their Services;
"Discount Structure"	means the Supplier commitment to provide a detailed discount documented approach applicable to offering discounts under the Framework Agreement and this Call Off Contract.

2. GENERAL PROVISIONS

2.1 This Call Off Schedule details:

2.1.1 the Call Off Contract Charges for the Services under this Call Off Contract; and

2.1.2 the payment terms/profile for the Call Off Contract Charges.

2.1.3 the invoicing procedure; and

2.1.4 the procedure applicable to any adjustments of the Call Off Contract Charges.

3. CALL OFF CONTRACT CHARGES

3.1 The Call Off Contract Charges which are applicable to this Call Off Contract are set out in Annex 1 of this Call Off Schedule.

3.2 The Supplier acknowledges and agrees that:

3.2.1 In accordance with paragraph 2 (General Provisions) of Framework Schedule 3 (Pricing), the Maximum Percentage Mark Up Rates set out in Annex 1 of the Framework Schedule 3 are the maximum mark-up rates that the Supplier may charge pursuant to any Call Off Agreement); and

3.2.2 The Parties acknowledge that Discount Structure as set out in Annex 2 to the Framework Schedule 3 shall be applied by the Supplier to this Call Off Contract.

3.2.3 subject to paragraph 7 of this Call Off Schedule (Adjustment of Call Off Contract Charges), the Call Off Contract Charges cannot be increased during the Call Off Contract Period.

4. PAYMENT TERMS/PAYMENT PROFILE

4.1 The payment terms/profile which are applicable to this Call Off Contract are set out in Annex 2 of this Call Off Schedule.

5. INVOICING PROCEDURE

5.1 The Customer shall pay all sums properly due and payable to the Supplier in cleared funds within thirty (30) days of receipt of a Valid Invoice, submitted to the address specified by the Customer in paragraph 6.5 of this Call Off Schedule and in accordance with the provisions of this Call Off Contract.

5.2 The Supplier shall ensure that each invoice (whether submitted electronically or in a paper form, as the Customer may specify):

6.2.1 contains:

(a) all appropriate references, including the unique (Purchase) Order reference number notified through the Customer's Accounts payable processes and

(b) a detailed breakdown of the Delivered Services, including the Milestone(s) (if any) and Deliverable(s) within this Call Off Contract to which the Delivered Services relate, against the applicable due and payable Call Off Contract Charges; and

6.2.2 shows separately:

(a) any Service Credits due to the Customer; and

(b) the VAT added to the due and payable Call Off Contract Charges in accordance with Clause 23.2.1 of this Call Off Contract (VAT) and the tax point date relating to the rate of VAT shown; and

6.2.3 is exclusive of any Management Charge (and the Supplier shall not attempt to increase the Call Off Contract Charges or otherwise recover from the Customer as a surcharge the Management Charge levied on it by the Authority); and

6.2.4 it is supported by any other documentation reasonably required by the Customer to substantiate that the invoice is a Valid Invoice.

5.3 The Supplier shall accept the Government Procurement Card as a means of payment for the Services where such card is agreed with the Customer to be a suitable means of payment. The Supplier shall be solely liable to pay any merchant fee levied for using the Government Procurement Card and shall not be entitled to recover this charge from the Customer.

5.4 All payments due by one Party to the other shall be made within thirty (30) days of receipt of a Valid Invoice unless otherwise specified in this Call Off Contract, in cleared funds, to such bank or building society account as the recipient Party may from time to time direct.

5.5 The Supplier shall submit invoices directly to:

Such addresses (electronic or postal) notified to the Supplier through the Customer's Accounts Payable processes.

6. ADJUSTMENT OF CALL OFF CONTRACT CHARGES

6.1 The Call Off Contract Charges shall only be varied:

6.1.1 due to a Specific Change in Law in relation to which the Parties agree that a change is required to all or part of the Call Off Contract Charges in accordance with Clause 22.2 of this Call Off Contract (Legislative Change);

6.1.2 where all or part of the Call Off Contract Charges are reduced as a result of a review of the Call Off Contract Charges in accordance with Clause 18 of this Call Off Contract (Continuous Improvement);

6.1.3 where all or part of the Call Off Contract Charges are reduced as a result of a review of Call Off Contract Charges in accordance with Clause and/or Clause 25 of this Call Off Contract (Benchmarking);

6.1.4 where all or part of the Call Off Contract Charges are reviewed and reduced in accordance with paragraph 8 of this Call Off Schedule;

6.2 Subject to paragraphs 7.1.1 to 7.1.4 of this Call Off Schedule, the Call Off Contract Charges will remain fixed for 4 (maximum) Contract Years.

7. SUPPLIER PERIODIC ASSESSMENT OF CALL OFF CONTRACT CHARGES

7.1 Every six (6) Months during the Call Off Contract Period, the Supplier shall assess the level of the Call Off Contract Charges to consider whether it is able to reduce them.

7.2 Such assessments by the Supplier under paragraph 8 of this Call Off Schedule shall be carried out on 1 September and 10 March in each Contract Year (or in the event that such dates do not, in any Contract Year, fall on a Working Day, on the next Working Day following such dates). To the extent that the Supplier is able to decrease all or part of the Call Off Contract Charges it shall promptly notify the Customer in writing and such reduction shall be implemented in accordance with paragraph 11.1.5 of this Call Off Schedule below.

8. IMPLEMENTATION OF ADJUSTED CALL OFF CONTRACT CHARGES

8.1 Variations in accordance with the provisions of this Call Off Schedule to all or part the Call Off Contract Charges (as the case may be) shall be made by the Customer to take effect:

8.1.1 in accordance with Clause 22.2 of this Call Off Contract (Legislative Change) where an adjustment to the Call Off Contract Charges is made in accordance with paragraph 7.1.1 of this Call Off Schedule;

8.1.2 in accordance with Clause **Error! Reference source not found.** of this Call Off Contract (Call Off Contract Charges and Payment) where an adjustment to the Call Off Contract Charges is made in accordance with paragraph **Error! Reference source not found.** of this Call Off Schedule;

8.1.3 in accordance with Clause 18 of this Call Off Contract (Continuous Improvement) where an adjustment to the Call Off Contract Charges is made in accordance with paragraph 7.1.2 of this Call Off Schedule;

8.1.4 in accordance with Clause 25 of this Call Off Contract (Benchmarking) where an adjustment to the Call Off Contract Charges is made in accordance with paragraph 7.1.3 of this Call Off Schedule [or]

8.1.5 on 1 October for assessments made on 1 September and on 10 February for assessments made on 10 March where an adjustment to the Call Off

Contract Charges is made in accordance with paragraph 7.1.4 of this Call Off Schedule; and the Parties shall amend the Call Off Contract Charges shown in Annex 1 to this Call Off Schedule to reflect such variations.

ANNEX 1: CALL OFF CONTRACT CHARGES (ALL PRICES QUOTED ARE NET OF VAT)

[REDACTED]

Note: An MOF will be provided for the above usage and Legal Ombudsman will only be bill for exact usage in arrears

Azure Hosting from previous months usage

[REDACTED]

Prices include support for:

- 1 Azure Subscriptions – Premier Tier (Networking, Maintenance tasks, Backups, Oncall, Patching, etc.)
- 1 Azure Gateway, Express route, Site to site VPN
- 1 WAF (Barracuda), 3 Firewall's (FortiGate 2 on premises, 1 azure), 1 site to site VPN, VPN service for End-users, 1 Azure Load Balancer
- On-premises network devices: 2 DMZ Switches, 2 Core switches, 12 normal Switches, 11 Aps.
- 29 Production VMs, 6 Non production VMs, 2 physical servers (DCs on prem)

Services included:

- Service Management, monthly reports, capacity management, security assessments, governance, av, fw, remote access, SLAs.
- Monitoring (active Monitoring, around 900 checks)
- CRM
- SharePoint
- SFTP
- File Server
- Reporting Services
- WAN Network
- LAN Network
- Domain and Identity management (AD, Adfs, Azure AD)
- Database
- Security assessment: 1 Yearly Pen Test preformed and Action plan elaboration.
- Microsoft Infrastructure and Azure Services (Environment management, capacity and security management).

ANNEX 2: PAYMENT TERMS/PROFILE

Pricing fixed for full 4-year (2+1+1) term unless reduced by agreement.

All prices are in Sterling and exclusive of VAT

[REDACTED]

[REDACTED]

Note:

- *Any non-BAU development days delivered must be accompanied by a signed Change Control Notice & Signed LeO Purchase Order (PO)
- *If Call-Off Development Services budget amount not reached in any year – this will NOT be charged to the Customer

Rate Card Support & Development Services

[REDACTED]

- Version 1 resources will be Quarterly in advance for Manage Service Support and monthly in arrears on a T&M basis for Development

- All charges are exclusive of travel/subsistence costs incurred by the Version 1 team
- All charges are exclusive of VAT
- Further roles not listed above can be provided upon request
- Rates are based on 7.5 hour working day
- Monthly invoices should be less than £70,000 including all invoiced hours, unless where agreed in advance in writing with the buyer

Travel and Subsistence

- Travel and subsistence will NOT be charged separately for the core Managed Service Provision and is included in the Service Management charge. This covers monthly and quarterly meetings between LeO and Version 1 relating to the service delivery
- Travel and Accommodation is payable at cost (plus VAT) for any additional contracted,non- BAU project activities applying the LeO policy for claim and payment of Travel and Subsistence.

Payment Profile

- Quarterly in advance for Managed Service Provision
- Monthly in arrears for Project Services

Drawdown Days

[REDACTED]

The Supplier is authorised to use up to 5 Drawdown days to deal with an incident, urgent or minor activity as required by the Operational Contract Manager.

The limit of 5 days per Drawdown is to be applied for any single piece of unscheduled work. Any further expenditure of effort on that work over the initial 5 days will require authorisation from the Customer's nominated Operational Contract Manager.

Such charges may be invoiced immediately by the Supplier if there are insufficient Drawdown days credited to the Customer's Service account at that time.

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:

9.2.1 during this Call-Off Contract, Subcontractors hold third party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000

9.2.2 the third-party public and products liability insurance contains an ‘indemnity to principals’ clause for the Buyer’s benefit

9.2.3 all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

9.2.4 all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

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 required

Schedule 4: Alternative clauses

1. Introduction

1.1 This Schedule specifies the alternative clauses that may be requested in the Order Form and, if requested in the Order Form, will apply to this Call-Off Contract.

2. Clauses selected

2.1 The Customer may, in the Order Form, request the following alternative Clauses:

2.1.1 Scots Law and Jurisdiction

2.1.2 References to England and Wales in incorporated Framework Agreement clause 8.12 (Law and Jurisdiction) of this Call-Off Contract will be replaced with Scotland and the wording of the Framework Agreement and Call-Off Contract will be interpreted as closely as possible to the original English and Welsh Law intention despite Scots Law applying.

2.1.3 Reference to England and Wales in Working Days definition within the Glossary and interpretations section will be replaced with Scotland.

2.1.4 References to the Contracts (Rights of Third Parties) Act 1999 will be removed in clause 27.1. Reference to the Freedom of Information Act 2000 within the defined terms for 'FoIA/Freedom of Information Act' to be replaced with Freedom of Information (Scotland) Act 2002.

2.1.5 Reference to the Supply of Goods and Services Act 1982 will be removed in incorporated Framework Agreement clause 4.2.

2.1.6 References to "tort" will be replaced with "delict" throughout

2.2 The Customer may, in the Order Form, request the following Alternative Clauses:

2.2.1 Northern Ireland Law (see paragraph 2.3, 2.4, 2.5, 2.6 and 2.7 of this Schedule)

2.3 Discrimination

2.3.1 The Supplier will comply with all applicable fair employment, equality of treatment and anti-discrimination legislation, including, in particular the:

- Employment (Northern Ireland) Order 2002
- Fair Employment and Treatment (Northern Ireland) Order 1998
- Sex Discrimination (Northern Ireland) Order 1976 and 1988
- Employment Equality (Sexual Orientation) Regulations (Northern Ireland) 2003
- Equal Pay Act (Northern Ireland) 1970

- Disability Discrimination Act 1995
- Race Relations (Northern Ireland) Order 1997
- Employment Relations (Northern Ireland) Order 1999 and Employment Rights (Northern Ireland) Order 1996
- Employment Equality (Age) Regulations (Northern Ireland) 2006
- Part-time Workers (Prevention of less Favourable Treatment) Regulation 2000
- Fixed-term Employees (Prevention of Less Favourable Treatment) Regulations 2002
- The Disability Discrimination (Northern Ireland) Order 2006
- The Employment Relations (Northern Ireland) Order 2004
- Equality Act (Sexual Orientation) Regulations (Northern Ireland) 2006
- Employment Relations (Northern Ireland) Order 2004
- Work and Families (Northern Ireland) Order 2006

and will use his best endeavours to ensure that in his employment policies and practices and in the delivery of the services required of the Supplier under this Call-Off Contract he promotes equality of treatment and opportunity between:

a. persons of different religious beliefs or political opinions
b. men and women or married and unmarried persons
c. persons with and without dependants (including women who are pregnant or on maternity leave and men on paternity leave)
d. persons of different racial groups (within the meaning of the Race Relations (Northern Ireland) Order 1997)
e. persons with and without a disability (within the meaning of the Disability Discrimination Act 1995)
f. persons of different ages
g. persons of differing sexual orientation

2.3.2 The Supplier will take all reasonable steps to secure the observance of clause 2.3.1 of this Schedule by all Supplier Staff.

2.4 Equality policies and practices

2.4.1 The Supplier will introduce and will procure that any Subcontractor will also introduce and implement an equal opportunities policy in accordance with guidance from and to the satisfaction of the Equality Commission. The Supplier will review these policies on a regular basis (and will procure that its Subcontractors do likewise) and the Customer will be entitled to receive upon request a copy of the policy.

2.4.2 The Supplier will take all reasonable steps to ensure that all of the Supplier Staff comply with its equal opportunities policies (referred to in clause 2.3 above). These steps will include:

a. the issue of written instructions to staff and other relevant persons
b. the appointment or designation of a senior manager with responsibility for equal opportunities
c. training of all staff and other relevant persons in equal opportunities and harassment matters

d. the inclusion of the topic of equality as an agenda item at team, management and staff meetings

The Supplier will procure that its Subcontractors do likewise with their equal opportunities policies.

2.4.3 The Supplier will inform the Customer as soon as possible in the event of:

A. the Equality Commission notifying the Supplier of an alleged breach by it or any Subcontractor (or any of their shareholders or directors) of the Fair Employment and Treatment (Northern Ireland) Order 1998 or

B. any finding of unlawful discrimination (or any offence under the Legislation mentioned in clause 2.3 above) being made against the Supplier or its Subcontractors during the Call-Off Contract Period by any Industrial or Fair Employment Tribunal or court,

The Supplier will take any necessary steps (including the dismissal or replacement of any relevant staff or Subcontractor(s)) as the Customer directs and will seek the advice of the Equality Commission in order to prevent any offence or repetition of the unlawful discrimination as the case may be.

2.4.4 The Supplier will monitor (in accordance with guidance issued by the Equality Commission) the composition of its workforce and applicants for employment and will provide an annual report on the composition of the workforce and applicants to the Customer. If the monitoring reveals under-representation or lack of fair participation of particular groups, the Supplier will review the operation of its relevant policies and take positive action if appropriate. The Supplier will impose on its Subcontractors obligations similar to those undertaken by it in this clause 2.4 and will procure that those Subcontractors comply with their obligations.

2.4.5 The Supplier will provide any information the Customer requests (including Information requested to be provided by any Subcontractors) for the purpose of assessing the Supplier's compliance with its obligations under clauses 2.4.1 to 2.4.5 of this Schedule.

2.5 Equality

2.5.1 The Supplier will, and will procure that each Subcontractor will, in performing its/their obligations under this Call-Off Contract (and other relevant agreements), comply with the provisions of Section 75 of the Northern Ireland Act 1998, as if they were a public authority within the meaning of that section.

2.5.2 The Supplier acknowledges that the Customer must, in carrying out its functions, have due regard to the need to promote equality of opportunity as contemplated by the Northern Ireland Act 1998 and the Supplier will use all reasonable endeavours to assist (and to ensure that relevant Subcontractor helps) the Customer in relation to same.

2.6 Health and safety

2.6.1 The Supplier will promptly notify the Customer of any health and safety hazards which may arise in connection with the performance of its obligations under the Call-Off Contract. The Customer will promptly notify the Supplier of any health and safety hazards which may exist or arise at the Customer premises and which may affect the Supplier in the performance of its obligations under the Call-Off Contract.

2.6.2 While on the Customer premises, the Supplier will comply with any health and safety measures implemented by the Customer in respect of Supplier Staff and other persons working there.

2.6.3 The Supplier will notify the Customer immediately in the event of any incident occurring in the performance of its obligations under the Call-Off Contract on the Customer premises if that incident causes any personal injury or damage to property which could give rise to personal injury.

2.6.4 The Supplier will comply with the requirements of the Health and Safety at Work (Northern Ireland) Order 1978 and any other acts, orders, regulations and codes of practice relating to health and safety, which may apply to Supplier Staff and other persons working on the Customer premises in the performance of its obligations under the Call-Off Contract.

2.6.5 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work (Northern Ireland) Order 1978) is made available to the Customer on request.

2.7 Criminal damage

2.7.1 The Supplier will maintain standards of vigilance and will take all precautions as advised by the Criminal Damage (Compensation) (Northern Ireland) Order 1977 or as may be recommended by the police or the Northern Ireland Office (or, if replaced, their successors) and will compensate the Customer for any loss arising directly from a breach of this obligation (including any diminution of monies received by the Customer under any insurance policy).

2.7.2 If during the Call-Off Contract Period any assets (or any part thereof) is or are damaged or destroyed by any circumstance giving rise to a claim for compensation under the provisions of the Compensation Order the following provisions of this clause 2.7 will apply.

2.7.3 The Supplier will make (or will procure that the appropriate organisation make) all appropriate claims under the Compensation Order as soon as possible after the CDO Event and will pursue any claim diligently and at its cost. If appropriate, the Customer will also make and pursue a claim diligently under the Compensation Order. Any appeal against a refusal to meet any claim or against the amount of the award will be at the Customer's cost and the Supplier will (at no additional cost to the Customer) provide any help the Customer reasonably requires with the appeal.

2.7.4 The Supplier will apply any compensation paid under the Compensation Order in respect of damage to the relevant assets towards the repair, reinstatement or replacement of the assets affected.

Schedule 5: Guarantee

Not required

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	For each Party, IPRs: • 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 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.
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	Data, Personal Data and any information, which may include (but isn't limited to) any: • 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	Default is any: • 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 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.
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	A force Majeure event means anything affecting either Party's performance of their obligations arising from any: • 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 The following do not constitute a Force Majeure event: • 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	Can be: • 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	Intellectual Property Rights are: • 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	For the purposes of the IR35 rules an intermediary can be: • the supplier's own limited company • a service or a personal service company • a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).
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	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:
	• 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:
	  ○ 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:
[REDACTED]

2.1 The contact details of the Supplier's Data Protection Officer are:
[REDACTED]

3.1 The Processor shall comply with any further written instructions with respect to Processing by the Controller.
3.2 Any such further instructions shall be incorporated into this Annex.

Descriptions	Details
Identity of Controller for each Category of Personal Data	**The Buyer is Controller and the Supplier is Processor** 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: ● Data relating to users of Legal Ombudsman IT Infrastructure.
Duration of the Processing	Contract Term plus Exit Period
Nature and purposes of the Processing	Personal Data is processed as part of administration of Legal Ombudsman's IT infrastructure. This will include login information, websites visited, session lengths, and IP addresses
Type of Personal Data	Name, IP Addresses, Websites visited
Categories of Data Subject	Staff

Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or	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

Member State law to preserve that type of data	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