
CORU Managed ICT Service Requirements and Specifications

Version:	0.1
Status:	Draft

Contents

1	INTRODUCTION	4
1.1	SERVICE RESOURCE EXPERTISE	6
1.2	IT SERVICE CONTINUITY MANAGEMENT	7
1.3	RESPONSE:.....	7
2	CORU LOCATIONS	8
2.1	ICT USERS AND LOCATIONS	8
2.2	DATACENTRE	8
3	BACKGROUND TO SERVICE REQUIREMENTS	9
3.1	CORU ICT GOVERNANCE MODEL	9
3.2	CURRENT CORU ICT ENVIRONMENT	9
4	MANAGED SERVICE REQUIREMENTS.....	11
4.1	SERVICE LEVELS	11
4.2	PERFORMANCE INDICATORS	14
4.3	LOCATIONS FROM WHICH SERVICE PROVISION SHOULD BE BASED	16
4.4	HOURS OF SERVICE	16
4.5	STAFFING PROVISION LEVELS	17
4.6	LEVEL 1 SERVICE DESK PROVISION	18
4.3	LEVEL 2 SERVICES PROVISION	20
4.4	LEVEL 3 SERVICES PROVISION	21
4.5	SERVICE DELIVERY MANAGER.....	23
4.6	MANAGED SERVICE PROVIDER'S ACCOUNT MANAGER	27
4.7	CORU INFRASTRUCTURE MANAGEMENT APPLICATION SUITE.....	27
4.8	EXISTING CORU PROJECTS.....	ERROR! BOOKMARK NOT DEFINED.
4.9	CORU CONTRACT MANAGEMENT AND SERVICE GOVERNANCE	28
4.9.1	<i>Service Desk</i>	28
4.9.2	<i>Service Management Process</i>	29
4.9.3	<i>Service Management & Reporting</i>	29
4.9.1	<i>Lessons Learned</i>	30
5	TRANSITION REQUIREMENTS	31
5.1.1	<i>Transition Guiding Principles</i>	31
5.1.2	<i>CORU Core Transition Requirements</i>	31
5.1.3	<i>Transition Management & Staffing</i>	32
5.1.4	<i>Service Handover & Contract Termination</i>	34
5.1.5	<i>Transition Costs</i>	34
6	TECHNICAL SERVICE REQUIREMENTS	35
6.1	LEVEL 1 AND LEVEL 2 SERVICE REQUIREMENTS	36
6.1.1	<i>Level 3 Service Requirements</i>	40
6.1.2	<i>Level 3 Services - Active Directory Management</i>	40
6.1.3		43
6.1.4	<i>Level 3 Services - Exchange Management</i>	44
6.1.5	<i>Level 3 Services - Server and Storage Management</i>	47
6.1.6	<i>Level 3 Services - Backup Management</i>	53
6.1.7	<i>Level 3 Services – LAN, Wireless & Firewall Management - List</i>	54
6.2.12	<i>Security - List</i>	58

6.2	ADDITIONAL EXPERTISE	62
	<i>Description</i>	62
	<i>Project Lead Description of Deliverables</i>	62
	<i>Project Services</i>	62
	<i>Customer Responsibilities</i>	63
7	CONTINUOUS SERVICE IMPROVEMENT	64
8	FORMAT OF TENDER RESPONSE	65
8.1	APPLICANT SUMMARY / COMPANY INFORMATION	ERROR! BOOKMARK NOT DEFINED.
8.2	ECONOMIC AND FINANCIAL STANDING	ERROR! BOOKMARK NOT DEFINED.
8.3	RELEVANT TECHNICAL AND PROFESSIONAL CAPABILITY	ERROR! BOOKMARK NOT DEFINED.
8.4	RESPONSE TO CORU SERVICE REQUIREMENTS	ERROR! BOOKMARK NOT DEFINED.
8.5	RISKS ASSOCIATED WITH THE SERVICE	ERROR! BOOKMARK NOT DEFINED.
8.6	COSTS	ERROR! BOOKMARK NOT DEFINED.
8.7	APPENDICES	ERROR! BOOKMARK NOT DEFINED.
9	COST REQUIREMENTS	66
9.1.1	<i>Introduction</i>	66
9.1.2	<i>Managed Services</i>	66
9.2	ADDITIONAL COSTS	67
9.3	COMPLETENESS OF COSTS	67
10	COMPLIANCE CHECKLIST	68
10.1	INSTRUCTIONS FOR TENDERERS	68
11	APPENDIX A CURRENT ENVIRONMENT	69
11.1	COMMS ROOM 5 TH FLOOR	69
11.2	COMMS ROOM 2 ND FLOOR	ERROR! BOOKMARK NOT DEFINED.
11.3	REVENUE DATA CENTRE	70
11.4	SOFTWARE:	70
12	APPENDIX B RACI	72
13	APPENDIX C ICT LIST OF CURRENT ONGOING PROJECTS	73
14	APPENDIX D CORU STANDARD TERMS AND CONDITIONS	74
15	APPENDIX E – CORU DIGITIZATION STRATEGY ..	75

1 Introduction

CORU is Ireland's multi-profession health regulator responsible for regulating health and social care professionals. It includes the Health and Social Care Professionals Council and the Registration Boards established under the Health and Social Care Professionals Act 2005 (as amended).

CORU's role is to protect the public through regulating the health and social care professions listed in the Health and Social Care Professionals Act 2005 (as amended).

To regulate the professions, CORU will:

- Set the standards that health and social care professionals must meet
- Ensure that the relevant educational bodies deliver qualifications that prepare professionals to provide safe and appropriate care
- Maintain and publish a Register of health and social care professionals who meet our standards
- Ensure that registered professionals keep their skills up to date by promoting Continuing Professional Development (CPD)
- Run Fitness to Practise hearings into the conduct and competence of a Registrant

CORU is made up of the Health and Social Care Professionals Council and 14 Registration Boards, one for each profession named in our Act.

The professions to be regulated are:

- Clinical Biochemists
- Counsellors and Psychotherapists
- Orthoptists
- Psychologists

CORU currently has registers open for the following professions:

- Dietitians / Dieticians
- Medical Scientists
- Occupational Therapists
- Optometrists and Dispensing Opticians
- Physiotherapists
- Podiatrists
- Radiographers and Radiation Therapists
- Social Workers
- Speech and Language Therapists / Speech Therapists
- Social Care Workers

Registers for the other professions will follow on a phased basis.

To facilitate CORU IT's Digital Strategy 2026 - 2028 (see Appendix E below) CORU wishes to tender for a managed service contract for their ICT Infrastructure.

The service provider will be expected to work closely and in partnership with the CORU ICT team.

While the CORU requirements are listed as CORU understands them at the point of writing, prospective service providers should expect a certain level of ongoing change throughout the lifetime of the contract and should specifically take the dynamic nature of this service into consideration when making their offering.

This tender is not divided into Lots so any prospective vendor must be capable of delivering the complete service requirements either from their own resources or, as lead contractor, utilising previously proven relationships.

While there is an existing incumbent supplier of some of the services detailed in this document, this RFT details a more comprehensive and structured approach to the delivery of ICT Managed Services and this should be noted by all prospective bidders.

While any questions and clarifications sought will be answered through the normal channels for such a tender, a Bidders Presentation will be held to outline the service as a whole and address any further questions arising. Bidders may also be invited to give a presentation on their submissions during the course of the evaluation process.

Working Arrangements

CORU have permanently altering their work practices to a blended approach between working from home and being present in the office. The successful Service Provider staff must be capable of engaging with this work arrangement if required and may be requested to work from home from time to time. The successful Service Provider will be responsible for all ergonomic and Health & Safety requirements in this eventuality. This arrangement will be agreed between CORU and the successful Service Provider. The successful Service Provider should note that any working from home arrangements must be agreed with CORU management.

Tenderers must be aware that the term "Onsite" in the document may refer to this blended approach. The tenderers must include in their response a description of how they can comply with this arrangement.

1.1 Service Resource Expertise

Prospective Tenderers must note that, while CORU accepts the need for ongoing staff training and the generation of suitable expertise, CORU expects that suitably trained and experienced staff form the core of the team assigned to them.

The tenderer must ensure that they can provide support across all elements of the Technical service requirements in line with agreed Service Levels.

The successful Service Provider will be expected to hold recognised certifications, qualifications and relevant experience in the areas of Windows Server, Active Directory, Exchange, Security, Networking and Firewall, Service Management, Storage and Backup, and, ideally, Agile Service Management. It is highly desirable that the personnel proposed by Tenderers have the certifications and experience set out in the table below.

Service	Qualifications	Experience
Windows Server Management	Relevant MCSE qualifications with Windows Server Component	>5 years
Active Directory Management	MCSE with MCP qualification in Active directory Administration & Design / Identity	> 5 years
Exchange Management	Microsoft MCSE Solutions Expert with designing and deploying Microsoft exchange server or MCSA Messaging	> 5 years
Network & Firewall	Network qualifications relevant to network estate and device vendors - Cisco CCNP R&S. Relevant Firewall vendor qualification.	> 5 years
Service Management	ITIL v4 Foundation minimum. Expert Level preferable Agile Service manager certification preferred	> 5 years
VmWare Management	Relevant VmWare qualifications	>5 years
Storage and Backup Support Management	Relevant Storage and Backup qualifications	>5years

It is expected that the Service Delivery Manager will have a minimum of 5 years' experience, with previous Team Leader experience and ideally would be qualified in at least two of the specialities listed above.

1.2 IT Service Continuity Management

CORU understands and accepts that the FTE (Full Time Equivalent) requirements listed below are small enough that it is unreasonable to expect that they shall be met by one individual in each area, but rather that they will form part of the workload for a team.

However, the Service Provider shall ensure that all members of its staff with responsibilities for dealing with CORU issues are aware of their individual assignments and duties.

The Service Provider shall furthermore ensure that all members of the assigned team are able to cover for each other and that CORU shall not see any reduction of service should any individual be unavailable.

Ideally, the Service Provider shall arrange for all members of the appropriate team to spend time on the CORU account.

The Service Provider shall explain how they propose to evaluate staff assigned to CORU, taking input from CORU into account.

1.3 Response:

The information contained in this RFT should be sufficient to facilitate responses from prospective bidders, but bidders should make sure they answer all the questions as specified in the Tender Response Document included below. Where there is uncertainty between the information included here and that in the sample response document, please answer the questions in the response document.

2 CORU Locations

2.1 ICT Users and Locations

CORU is located in Smithfield, Dublin and has approximately 100 staff at this location. There are a total of approximately 350 associate additional users located in remote sites nationwide, but their interactions with CORU do not generally require access to back-end systems.

2.2 Datacentre

CORU hosts its primary centralised servers in a resilient Datacentre facility in the Revenue Commissioners, Kilmainham. The facilities at their office in Smithfield, Dublin houses their Failover and backup services.

The successful tenderer will be expected to provide Level 2 support to the CORU ICT Unit based in the office at Smithfield. Though most work will be remote support there will be an occasional need for work to take place in either Smithfield or Kilmainham.

While Services are to be delivered to end-users in all locations, to home workers and those staff travelling or remotely stationed it is expected that such services will be minimal and can usually be delivered remotely.

3 Background to Service Requirements

3.1 CORU ICT Governance Model

CORU has established a project management board to oversee the implementation, management and performance of the Managed Service. Day to day operational management will be the responsibility of the service provider via an experienced ICT Service Delivery Manager. This manager will liaise with the CORU ICT Service Delivery Manager for all levels of support with escalation, if required, to the Head of Digital and Quality Systems.

3.2 Current CORU ICT Environment

CORU's physical infrastructure is generally standardised and centrally managed, broadly following ITIL processes for services and Prince2 for project implementation.

The hardware, software and cloud components which make up the physical infrastructure have been standardised, in so far as possible, to allow for the build of a homogenous IT system. Standardisation will continue to be an important principle in the evolution of the infrastructure and will be a core requirement in the management of these environments by the selected provider.

All on-premise ICT infrastructure is owned by the CORU Digital and Quality Systems Department and is the responsibility of the ICT Department. No infrastructure can be purchased or connected to the CORU ICT network without the specific approval of the ICT Department.

CORU has a number of ICT environments which are managed through a combination of CORU Internal ICT staff or existing service providers.

Currently, the server infrastructure is hosted between the Revenue Data Centre (DC1) and Smithfield (DC2). All WAN connections between the two sites are through Government Networks.

The ICT environments which form the basis of this tender document are described in the Appendices below, along with a description of the services required for each which can be found in Section 6 below. Prospective suppliers should note that while there are a number of hardware and software vendors, Microsoft, and DELL are currently predominant and the environment is largely homogenous. See Appendix A for more details.

Prospective service providers should pay special attention to the need for a comprehensive transition plan in their tender document.

CORU have a 365 presence and utilise the Revenue Data Centre as a private cloud running the “Production systems” from there and having Smithfield running in a mirrored setup to facilitate Failover and also running Veeam Backup to provide a 3-2-1-1-0 Golden Backup rule.

While it is not envisaged that CORU will be moving entirely to the Cloud we do have a number of key systems running in a SaaS environment. Tenders should therefore include a summary of their exposure to and support of private cloud type infrastructure models and support of SaaS applications within a Managed Service context (Networking, Identity Management etc.).

There is a variance from the purest interpretation of ITIL within CORU. For example, on change management, individual manager sign-off rather than a CAB decision is currently considered sufficient. In addition, Requests are not all predefined.

Any request looking for a service within the bounds of normal operations for service areas covered by the services in the contract is treated as a Request and taken on its individual merits as to whether it is feasible or desirable.

It is expected that the successful tenderer will work with CORU to help implement a more structured, ITIL based, Agile managed service. Tenderers should be aware that this will involve a level of behaviour change within CORU.

Any further details of the current technical environment will be made available through the forum of clarifications submitted in relation to the tender or at the Bidders Presentation.

4 Managed Service Requirements

There will be a Bidders Presentation to outline clearly the expectations from the contract and to help clarify any questions relating to the existing technical or operating environment, or clarification required on the nature of the services required.

4.1 Service Levels

CORU ICT is moving to a new ticketing system build into it's current RMM / asset management system, NinjaOne, as this system controls endpoint management, patching for both laptops and servers and security management using Crowd Strike Falcon, we expect this to be take this into account. CORU are not willing to consider the adoption of other ticketing systems, as all helpdesk data goes towards helpdesk support library.

For the avoidance of doubt, tenderers should be aware that all data relating to calls logged will remain the property of CORU, and this should be acknowledged by all bidders.

CORU will look to implement Ticket priorities on the following matrix:

		Impact			
		Whole Organisation	Whole Business Unit	One Location	One Person
Urgency	Unable to work	P1	P1	P2	P3
	Severe impact with workaround	P2	P2	P3	P4
	Restricted use	P2	P3	P3	P4
	Low impact/question	P4	P4	P4	P4

Required Response & Resolution times

Attribute	Priority	Mandatory Response Time	Target Resolution Time
Incident Analysis and Assignment	Priority 1	Within 15 minutes	4 Hours
	Priority 2	Within 30 minutes	Same working day
	Priority 3	Within 2 hours	Next Working Day
	Priority 4	Within 4 hours	Second next working day
Service Desk Update Frequency	Priority 1	30 minutes	
	Priority 2	2 hours	
	Priority 3	4 hours	
	Priority 4	8 hours	

Prospective Suppliers should note that the times referred to above are elapsed times, not cumulative working times.

Response Time refers to the person who logged the call receiving a communication from the Service Desk that the ticket has been assessed, categorized or recategorized if required and assigned to an appropriate resolver.

There may also be a VIP service operated for approximately 10 users.

Prospective Suppliers should also note that there is a business expectation that all systems will be 100% available during the core service hours listed above and where that is not achieved both the Managed Service and CORU will have an understanding of the reasons and all parties will work together to remedy issues as quickly as possible.

We expect the Managed Service Provider to operate to a Service Level Agreement (SLA), with, at a minimum, the KPI's listed below. Suggestions for additional metrics in addition to those below will be welcomed and considered. The objective of the SLA is to ensure agreement to and monitoring of an optimal level of ICT service, in close co-operation between CORU, the selected Managed Service Provider and existing external suppliers.

The SLA will cover the management of:

- Level 2 services – those ICT services which will be provided directly to the selected managed service provider from the CORU Ticketing system eg. Service Desk escalated tickets.
- Level 3 services – those ICT services which will be provided by the selected managed service provider in operation and support of the ICT

infrastructure i.e. technical support services, continuous service improvement and delivery of selected business or technical projects.

It is vital that prospective service providers note that the responsibility for measuring and managing end-to-end resolution times, and subsequent adherence to the SLA, will lie solely with the Service Provider, where the Service Providers own staff perform the resolution. In instances where the final resolution is performed by CORU staff or a Third Party, best endeavour will be made by the Service Provider ensure that they are not the cause of avoidable delay e.g. in diagnosing issues accurately or in ticket handling.

The Service Level Agreement will be:

- a) Between CORU and the Managed Service Provider***
- b) Based on the CORU Internal SLA and***
- c) Operation Level Agreements to be drawn up by the Managed Service Provider and any Third Parties (including CORU ICT Department)***

The selected service provider will assume responsibility and accountability for the availability, performance, and reliability of each of these CORU services along with the accompanying ICT processes. The provider will take responsibility for administration, monitoring, maintenance, support and disaster recovery of these ICT environments.

4.2 Performance Indicators

CORU reserves the right for KPIs to be amended by CORU to improve service measurement or/and address undesirable or unanticipated behaviours encouraged by KPIs or PI's.

Key Performance Indicators

1. Infrastructure Stability

All major Infrastructure components (virtual and physical servers, ESX hosts, Storage, Switches, Firewalls, Wireless system, Fileshares, Mail, Teams, SharePoint servers and systems) Uptime $\geq 99.99\%$ during business hours, excluding planned outages.

2. Service Desk escalated Incidents and Requests

These apply only to the areas resolvable by the Managed Service. It is not the intention to make the Managed Service Provider accountable for 3rd parties outside of their control e.g. Managed Print Services, Managed Mobility services, 3rd party application, software or hardware support or CORU ICT Dept.

Adherence to the Response and Resolution targets outlined above $\geq 85\%$ (that refers to the P1's, P2's etc. Urgency/Impact matrix)

- ✓ MTTR for Incidents - 1.5 days
- ✓ MTTR for Requests - 2.5 days for requests that do not require escalation to other Resolver groups.
- ✓ FCRR First Contact Resolution Rate (Incidents and Requests combined) – 70%
- ✓ FLRR First Level Resolution Rate (Incidents and Requests combined) - 75%

3. Speedy resolution of critical issues that prevent users from working, to include the following:

- ✓ Email Server flow
- ✓ AD Management
- ✓ VPN access issues

5. Patching compliance rates for patching monitoring (Patching is automated through RMM)

- ✓ Server Patching $\geq 99\%$ Compliant
- ✓ Desktop/Laptop patching $\geq 95\%$ Compliant. Devices not powered on or recently connected via VPN will be discounted.

6. IT Asset Management Inventory Accuracy

- ✓ The Annual physical audits variance with where an asset is reported to be $\leq 2\%$
- ✓ The status (active or inactive) $\leq 2\%$ variance
- ✓ The retrieval rate of assets in the Asset Management system before escalation to the CORU SDM team. $\geq 90\%$

7. Customer Satisfaction

Customer Satisfaction rating as reported in follow-up surveys after ticket closures should not drop below 85% and each dissatisfied response will be followed up individually by the Managed Service SDM to understand the cause of the dissatisfaction. Proposals for future improvement of the Service to address issues raised well then be considered and actioned if appropriate.

Performance Indicators

The following need to be monitored and reported on but incur no financial penalty

Incident Re-Assignments - average re-assignments per ticket.

Incident Re-Assignments to CORU Staff - average re-assignments per ticket to a CORU Resolver.

Incorrectly Assigned Incidents – Monitored by the Quality tab in Ticketing System

Aging Incidents and Requests by Priority and Age – This will be an indicator of tickets not being ignored after the SLA has been breached.

Informationally, reporting on tickets in CORU Resolver Groups may also be useful in understanding the ICT Service CORU delivers to its users and insights gleaned from such reporting may lead to improvements in process across the ICT Service as a whole.

In addition to the KPI's above, the selected service provider will be expected to demonstrate how they will manage and evaluate the performance of assigned staff on an ongoing basis.

The selected service providers must nominate a Service Delivery Manager, who will be the primary point of contact between CORU and the vendor. This manager will be responsible for the deployment of assigned resources in conjunction with CORU and will be solely responsible for the performance of the vendor's staff. CORU reserves the right to highlight staff performance that is consistently below the level required and the vendor must detail actions taken to remediate staff performance up to and including re-assignment of staff.

The selected service provider is also expected to provide a project service. See Project Services requirement below in section 6.2 for more detail.

The selected service providers are expected to demonstrate how they would drive value and continuous improvement throughout the lifetime of this contract.

4.3 Locations from which service provision should be based

Environment	Description	Location
Service Desk (escalated)	Escalated Level 2 Service provision	To be provided from service provider's premises which must be located within the EEA.
Level 3	All Sysadmin's and Network resources	To be provided from service provider's premises which must be located within the EEA.
Service Delivery Manager		Vendor Discretion

4.4 Hours of service

CORU require:

- Level 2 services should be available from 09:00 to 17:15 Monday to Friday.
- Level 3 services should be available from 08:30 to 17:30 Monday to Friday.

From time-to-time CORU may require that the service provider provide support beyond the core hours however such occasions will be limited and within reason (for example system upgrades, testing etc.). CORU would expect these services to be covered without CORU incurring extra charges. Potential service providers should suggest methods by which this aim can be achieved.

4.5 Staffing Provision Levels

The overall approach will not be to specify how many of each level of technician/resource are required, but to provide information on the volume and nature of tickets and allow Managed Service providers to assess what they feel are the appropriate staffing levels. Marks will be awarded based on both cost and staffing levels, with a view to achieving value while not penalising a submission because a better but more expensive service is proposed, if it is felt that the cost will deliver sufficient value to the organisation.

The existing staffing levels are provided as a reference point only, with the exception of L1 Service Desk escalated support, where the staffing levels specified are baseline levels, and the L3 Project resource, where it is felt that 1 FTE is a minimum requirement which can be supplemented by recourse to the rate card requested in Section 6.3 if the workload or priority of projects justifies the additional expense. This will be determined by agreement between the customer and provider.

Network resourcing, in particular, may require more resources or resources with a higher skillset as it has been a bottleneck historically and as more services move towards the edge of the network, complexity and demand may grow over the lifetime of the contract.

A further consideration is consistency of staff across the contract. ***A core of people who build familiarity with the environment and relationships with the Digital and Quality Systems Department and the organisation as a whole are considered essential to the success of the endeavour.***

Minimum levels of educational achievement, English language proficiency and/or years of experience are specified for each resource level. CORU requires a brief CV for each proposed resource that will work on the contract.

CORU reserves the right to request a different resource for a specific role at the commencement of the contract or at any time after that. CORU reserves the right to have a resource replaced on the account at any time and without quibble, a suitable and similarly experienced resource being provided by the Managed Service partner for approval by CORU by means of CV and/or interview.

CORU requires potential service providers to demonstrate the standards used by them when evaluating the English language skills of Customer facing staff in general, as well as those that would be assigned to the CORU account.

The service provider must explain their approach to routine and unavoidable unavailability of resources due to, for example, training courses and annual leave, in order to not impact on services to CORU.

A full description of the current operating environment and the responsibilities of both CORU and the Managed Service partner are provided the appendices below.

4.6 Service Desk Support Provision

CORU's Service Desk acts as the hub of ICT support. The Service Desk is managed by 2 CORU ICT staff. In addition to resolving a minimum of 75% of all issues within remit at this first point of contact, the Service Desk will act as the filter for all issues that are passed to Level 2 or Level 3, Service Provider NOC or Third-Party services for resolution. ***The Service Desk will be the owner of all issues and will manage incidents from initial logging to closure.***

CORU anticipates that staff from the CORU ICT team will man the Service Desk though, from time to time, the Managed Service Provider may have to supplement the CORU staff. It is anticipated that CORU will provide 2 FTEs for this role.

Supplementary staff may be housed by the supplier, rather than at a CORU site. Site to site VPN connectivity and End User PC can be provided by CORU. Access to the Ninja One RMM system will be provided to aid support where required.

The Service Desk will handle any issues raised by telephone or Email or via a Portal by any of the CORU users. Sample call volumes can be seen below:

Tickets to the ITHelpDesk Jan 24 – Nov 25			
	2024		2025
January	141	January	266
February	137	February	169
March	118	March	185
April	140	April	200
May	118	May	211
June	157	June	228
July	129	July	200
August	233	August	190
September	277	September	197
October	224	October	395
November	330	November	314
December	236		
Total	2240		2555

Approximately 85% of calls can be regarded as P3 or P4, while the remainder are primarily P2 in nature. CORU has had less than 15 P1 calls logged in the period detailed above.

The general tasks of the ICT Service Desk are to:

- Receive and record all tickets issued by End Users, which deal directly with incidents, problems, requests, changes and queries.
- Log all calls into the call logging system.
- Perform 'first-pass' issue identification and, if possible, resolution
- Monitor and forward all incidents and/or requests for change according to agreed service levels.
- Keep End Users informed on status and progress until the incident is resolved.
- Proactively inform users regarding known overall problems (e.g. "hot news") via appropriate channels.

*Please note that these are CORU best estimates of the FTE requirements. It is ***entirely the responsibility of the Service Supplier to provide adequate resources to meet CORU service requirements.***

4.3 Level 2 Services Provision

The table below details the Level 2 services required within the scope of the managed service.

Environment	Description	Expected FTE allocation	Minimum Educational Attainment/Experience
Remote Support	Remotely manage escalated issues relating to Level 2 Services.	0.5 FTE	Level 6 in an IT discipline and 1 years' experience or 2 years relevant industry experience and relevant certifications (e.g. CompTIA) ITIL certification.

The general tasks of the ICT Service Desk are to:

- Receive incidents and requests from CORU and the Service Desk where the ServiceDesk cannot resolve the ticket.
- Coordinate onsite services with 3rd parties and escort to correct equipment as necessary.
- Assist with hands-on and smart hands support (through Teams) as required.
- Provide urgent support to VIPs and assistance for Audio-Visual equipment. E.g., in Conference Rooms. In conjunction with on-site CORU ICTG staff complete routine checks of audio-visual equipment as a proactive measure.
- Asset management and inventory control.
- Assisting users with 365 tools, 3CX soft phone system and IT requirements for events.

*Please note that these are CORU best estimates of the FTE requirements. It is ***entirely the responsibility of the Service Supplier to provide adequate resources to meet CORU service requirements.***

TUPE may apply between staff working for an incumbent provider and any new provider. The onus is on potential bidders to determine if this is the case. CORU will provide data on request to assist in making this determination and the extent of any potential obligation.

No CORU staff will be moving to the selected vendor so TUPE will not apply to CORU staff.

4.4 Level 3 Services Provision

The table below details the Level 3 services required within the scope of the managed service.

Environment	Description	Expected FTE allocation	Minimum Educational Attainment/Experience
Senior Sys Admin	Remote support for issues assigned from the Service Desk	0.2 FTE	Level 6 in an IT discipline and 6+ years relevant industry experience or 8 years relevant industry experience. Industry certifications such as MCSE and VCP.
Senior Network Admin	Remote support for issues assigned from the Service Desk	0.1 FTE	Level 6 in an IT discipline and 6+ years relevant industry experience or 8 years relevant industry experience. Industry certifications such as MCSE and CCNP/CCIE, Fortigate, Juniper certifications.
Security Officer	System wide support to ensure the integrity of all CORU ICT systems	0.2 FTE	Level 6 in an IT discipline and 6+ years relevant industry experience or 8 years relevant industry experience. Industry certifications such as MCSE and VCP.

Details of the Level 3 services required within the scope of the managed service are provided in Section 6, along with a detailed description of the existing environment and external support resources available to the Managed Service provider. The service provider will be expected to provide administration, technical support and maintenance for these environments. Tenders should demonstrate how they will proactively and constructively support the rapid take-on of new or upgraded infrastructure where the project is delivered by a third party.

CORU delivers a large number of mini-projects to support its diverse end-user base.

The change management process is usually sufficient governance for these. Formal Project Management, where required, will be provided by CORU.

The suggested definition of projects appropriate for this resource is Change Requests and Projects expected to require 10 effort days or less which do not fall into the scope of the Business-As-Usual services outlined in Section 6 or more than 15 concurrent or sequential requests requesting the same or a related deliverable. The priority given to delivering these projects will vary depending on the business demands.

A process for scoping and sizing of the project will be undertaken before starting. The skill set requirements, effort estimates and potential impacts to the service as a whole will be examined and agreed before commencement.

The volume of project work may have peaks and troughs and an additional resource may be required for periods. The cost of this additional resource will be stipulated in the rate card detailed in Section 6.3.

It is ultimately the service provider's responsibility to provide the services required by the SLA and to assign the resources to meet the SLA. Multiple requirements can be met by an individual technician. Escalation resources within the Managed Service Provider available to Level 3, such as Technical Architect, Database Administrator, Network Architect, DevOps and Process Automation should be available to advise on both strategic and operational matters at no cost to CORU. It is not the intention that these escalation resources deliver substantial projects without recourse to the Rate Card (see section 6.3) but they are expected to be available where Level 3 need to escalate on operational issues or where the work in the Project queue requires their input.

Note: Volume of ongoing projects will mean that estimates above are subject to change but can be used as a baseline guide. The Rate Card requirement allows for an increase in Project resources for a time by mutual agreement between CORU and the Provider.

Further details of the service elements are provided in the detailed technical requirements sections below.

4.5 Service Delivery Manager

Environment	Description	Expected FTE allocation	Minimum Educational Attainment/Experience
Service Delivery	See below	0.1 FTE	ITIL Certification > 5 years experience

A dedicated Service Delivery Manager is required and a particular resource should be specified. This manager will be responsible for the deployment of assigned resources in conjunction with CORU and will be solely responsible for the performance of the vendor's staff. Their role will include but not be limited to:

- Responsibility for the service provision and provide a primary point of contact to the Customer for all service-related issues.
- Driving implementation and on-going adherence to the ITIL processes.
- Managing service delivery to ensure the maintenance of a fully functional, reliable and secure ICT environment and service desk
- Ensuring a co-ordinated approach is taken to the delivery of all services including the management of interdependencies and risks.
- Ensuring incidents, major or otherwise, are resolved according to agreed service levels.
- Delivering a programme of continuous service improvements.
- Where necessary co-ordinating the activities between the managed service team and third-party vendors in the resolution of incidents.
- Management of change to the assigned live environments while maintaining the accuracy of associated systems documentation.
- Responsibility for ensuring the timely and efficient implementation of Contractor implemented changes, including liaising with customer and third-party staff involved in change implementation.
- Reporting on service delivery through the provision of monthly service review reports and major incident reports as agreed.
- Providing advice and guidance on any matters relating to the CORU ICT environment.
- Maintaining end-user satisfaction with the service delivered to the user community and the business in line with service levels. This will include the management of complaints and acting as an escalation point when appropriate.
- Addressing implementation of recommendations arising from audits within the team capacity and skill sets.

Meetings

The Service Delivery Manager will be responsible for compiling these reports, hosting the meetings and maintaining minutes for these meetings.

Meeting Title	Purpose	Frequency	Attendees	Owners
Service Review	Review of monthly SLA/KPIs and Operational aspects of the Service, including Continuous Service Improvement measures.	Monthly	Contractor Service Delivery Manager Contractor Account Executive Customer Head of ICT Customer TSM Customer SDM Customer Security Manager	Contractor
Quarterly Service Overview and New Developments	Discussion of issues with all local stakeholders, updates on company strategy effects on IT and service delivery, discussion of Continuous Service Improvement measures.	Quarterly	Contractor Service Delivery Manager Contractor Account Executive Customer Head of ICT Customer TSM Customer SDM Customer Security Manager	Contractor
Problem/Change Management review	Discussion of Problems and Change Requests and frequently also topical technical issues of the day.	Fortnightly	Customer Infrastructure Team Customer Service Delivery Team Customer Security Team Contractor L3 team	Contractor
Operational Updates	Service updates for week ahead and topical technical issues.	Weekly	Customer TSM Customer SDM Contractor SDM	Contractor

Meeting Title	Purpose	Frequency	Attendees	Owners
Service Priorities	Discussion of Problems and Change Requests and frequently also topical technical issues of the day.	Fortnightly	Customer Infrastructure Team Customer Service Delivery Team Customer Security Team Contractor L3 team	Contractor
Review of Shared Risk Log	To identify and mitigate or accept shared risk between Contractor and CORU.	Quarterly	Contractor SDM Customer Infrastructure Team Customer Applications Team Customer Security Team Customer Service Delivery Team Customer Research and Innovation Manager Customer Head of ICT	Contractor

Reporting

The Service Delivery Manager will be responsible for providing the following reports.

Report Name/Purpose	Frequency	Report Availability
Monthly report – this report will summarise the activity and service delivery for the previous calendar month.	Monthly	5 working days prior to service management review or within 5 business days of month end
Quarterly Report - including details on change records, calls, response and fix times, trend analysis, recommendations, actions and performance, specific service improvements planned and delivered and any commercial issues	Quarterly	Within three weeks of the quarter's end
Major Incident Reports	Variable	3 days for interim (high level) report, 1 week for detailed report, 2 weeks if depending on third party.
Minutes of ICT Support Meetings	Weekly	
Minutes of Service Review Meetings	Monthly	
Minutes of Service Overview meetings	Quarterly	
Ad-hoc reports via SysAid – to be produced as required by the Customer	As Required	As Required, run by the Customer personnel
Ad-hoc reports by agreement – produced by the Contractor	On agreement	On agreement
Quarterly Report - including details on change records, calls, response and fix times, trend analysis, recommendations, actions and performance, specific service improvements planned and delivered and any commercial issues	Quarterly	Within three weeks of the quarter's end,
Major Incident Reports	Variable	3 days for interim (high level) report, 1 week for detailed report, 2 weeks if depending on third party.
Minutes of ICT Support Meetings	Weekly	
Minutes of Service Review Meetings	Monthly	
Minutes of Quarterly meetings	Quarterly	

Annual Strategic Overview, encompassing the market in general terms and relevant threats and opportunities.	Annual	On the anniversary of contract commencement.
Ad-hoc reports via ATS – to be produced as required by the Customer	As Required	As Required, run by the Customer personnel
Ad-hoc reports by agreement – produced by the Contractor	On agreement	On agreement

Throughout the duration of any contract awarded as a result of this procurement, CORU may undertake or commission a third-party organisation to undertake reviews and audits of any or all of the services and/or facilities provided by the successful service provider. The successful service provider will be expected to facilitate and co-operate fully with any such audits and to provide access to any facility, information or records required for the purpose of undertaking the audits.

The successful service provider will be required, on request by CORU, to arrange for the timely implementation of any recommendations arising from such audits. Service providers must specifically confirm their acceptance of this condition.

4.6 Managed Service Provider's Account Manager

The selected service provider is expected to nominate an Account Manager (in addition to the Service Delivery Manager), who will be expected to attend the monthly service reviews referred to above and who will act as the primary contact to CORU on all contractual, as opposed to technical, issues.

The selected service providers will be expected to use recognised best practice guidelines (e.g. ITIL) in delivering this service.

4.7 CORU Infrastructure Management Application Suite

The list of key applications below are used to operate and manage the entire CORU ICT infrastructure. CORU have support agreements in place with external service providers covering some of these infrastructure applications, as detailed below, and it is envisaged that the successful service provider will liaise directly with these service providers. Service Providers may change over time through the normal cycle of contract renewals.

- Microsoft SCCM
- Barracuda Email Archive
- Ninja One RMM
- ManageEngine Log360
- AD Manager
- vCenter

- Fortinet VPN Authenticator
- CrowdStrike Falcon complete
- Veeam v13 Backup and Replication

4.8 Areas of importance for CORU ICT

There are a number of areas in CORU ICT planning where we wish to focus in the short to mid-term, these are broken down into the following groups:

- Automation and AI
- Cybersecurity
- Data Warehousing

We would expect the selected service provider to have “Champions” for each area who can advise and guide us taking into account that we are a Public Sector body and must adhere to all relevant policies and procedures.

4.9 CORU Contract Management and Service Governance

CORU will nominate a primary contact who will be responsible for managing the relationship with the chosen service provider. Service providers should note that while ultimate responsibility will lie with the ICT Manager, CORU will manage this contract using the ICT management team.

Note: CORU reserves the right to implement service credits and Vendors are required to suggest typical service credits as part of their proposal.

4.9.1 Service Desk

The ICT service desk is an integral part of this tender and the present ICT Service Desk will continue to operate through the existing service provider until any handover required is complete. Most activity occurs between 09:00 and 17:00 but coverage from 08:30am to 5:30pm is required.

4.9.2 Service Management Process

Prospective service providers should indicate how they intend to approach the following processes in the context of this service:

- Availability Management
- Resource Management
- Request Fulfilment
- Incident / Problem Management
- Change Management
- Continuous Service Improvement
- Capacity Management
- Configuration Management
- All other ITIL processes

4.9.3 Service Management & Reporting

The service provider must provide a single point of contact, the Service Delivery Manager, who will be responsible for delivery of the contracted managed service. The Service Delivery Manager will facilitate monthly operation reviews, and monthly reporting in compliance with the service levels agreed.

The selected service provider will be required to produce monthly reports and hold monthly reviews with the CORU Contract Management team to evaluate the effectiveness and quality of the service provided with a focus on continuous improvement. CORU will expect that where service gaps exist the service provider will proactively identify service improvement initiatives, both process-related and technical.

CORU expect that at a minimum the service provider will produce service reports pertaining to key process indicators on primary back office systems and services such as for example; Servers, Exchange, Citrix, Networking, Active Directory, Linux, Lync, Oracle Database, Veeam etc.

- Monthly Reporting Requirements: KPI's (Key Performance Indicators), PI's (Performance Indicators) and SLA's to be reported on monthly. System performance, capacity statistics, quality metrics, user satisfaction, trend analysis, calls, complaints, problems, major incidents, patching reports and any further agreed useful metrics.
- Quarterly Reporting Requirements: Creation of Managed service performance report including details on change records, calls, response and fix times, trend analysis, recommendations, actions and performance, specific service improvements planned and delivered and any commercial issues.

- Any major outages that have occurred in the previous reporting period should be detailed along with a Lessons Learned report.
- The monthly report should also include progress and suggestions on continuous improvements.

A template for monthly service reporting will be agreed with the successful bidder but is expected to broadly replicate the sample provided in Appendix D, at a minimum. Any suggested improvements or additional useful metrics the Provider suggests will be welcomed for consideration.

The current monthly reports should include the following as a base:

- SLA/KPI/PI results with narration, including explanations on SLA/KPI breaches
- Summary of priority 1 incident resolution details (note P1s will also drive a major incident report at time of incident).
- Summary of YTD change requests
- Summary of YTD problems
- Aged ticket quantities
- Top 10 categories over past 3 months
- Top 10 ticket loggers over past 3 months
- Tickets by month (& department if available)
- Ticket priority by month
- Average time to resolve by month
- Average time to respond by month
- Ticket reassignment
- Tickets by source (Portal, Service Desk, email, etc.)
- Total time spent waiting on user response by month
- Virus detection by month
- Virus detection by type
- Virus tickets logged to service desk by month
- Top 5 viruses over past 12 months
- Viruses by user by month (scheduled/user initiated scans)
- Security incidents by month
- Managed software product license usage
- Server and Infrastructure Patching summaries
- Backup failure rates
- Capacity management reports
- Technical risk areas (e.g. server ages, capacity issues)
- Continuous Improvement (e.g. log of opportunities / root cause analysis complete identified this month for review by steering group).

4.9.1 Lessons Learned

Any major outages that may have occurred in the previous reporting period must be detailed along with a 'Lessons Learned' report. For a major outage, an incident report must be delivered by the Service Provider within two working days of the incident. It must outline the incident, the cause, resolution and any recommendations / follow up action required.

In addition to the provision of sample SLAs and KPIs, CORU's Service Delivery management requirements and Lessons learned should be demonstrated in the previous experience of similar sized projects and also a response with sufficient detail that outlines the providers general approach

5 Transition Requirements

A Transition plan to take on service and another to exit the service will be required from the successful providers. Special attention should be paid to the Transition plan so as to ensure no disruption to CORU end-users.

Potential vendors should note that costs associated with Transition at the start of the service should be identified and these costs will be excluded when total costs are being evaluated.

5.1.1 Transition Guiding Principles

The transition plan must include the transition of:

- Services currently managed by existing service providers - see RACI matrix in Appendix B.
- Additional services currently provided in whole or in part by CORU staff that will shift to the Managed Service.
- Services listed in the Managed Service Requirements in section 4.
- Any new projects which are complete or incomplete prior to the commencement of the new service. Updates on these projects will be provided as required. For a list of current ongoing projects see Appendix C

A smooth transition of service provision from the current arrangements to the new contract is essential. There must be no disruption to CORU service provision and users should not be aware of any changes apart from improvements. The key criteria for the provision of the Transition Services, and hence for the evaluation of the service provider's Tenders, are:

- The achievement of a seamless transition from the existing to the new service arrangements
- Communication with end-users
- Documentation of existing and new services
- Training of proposed staff in the specifics of CORU operations and Knowledge Management.

5.1.2 CORU Core Transition Requirements

If necessary, the selected service providers will be expected to enter into discussions with both the CORU Digital and Quality Systems Department and our current service providers. The provision of the services sought under this tender (following the

transition period) will become the responsibility of the newly appointed service providers. During the transition period the service provider must make adequate arrangements for the transfer of all relevant information from the current service providers and CORU, including training to cover organisation awareness, overview of main business and technical applications and any other pertinent information to the new service provider; and ensure CORU data is protected and not disclosed.

CORU expects that the transition of services will be planned and managed using a recognised project management methodology e.g. PRINCE2 or an equivalent recognised methodology.

The service provider must outline an indicative implementation plan for the transition services as part of their Tenders. It is essential that the transition exercises be completed by 30 December 2026. Please note that all responses to this tender must also include a transition plan for exiting the service, in addition to a plan for entering it.

CORU will expect the selected Service Providers to provide the following information when detailing their response to service transition

- Their experience and track record in delivering the type of transition services sought in this Invitation to Tender
- The key personnel who will be responsible for undertaking the transitions including details of their previous experience in delivering such projects
- Lessons learned from previous Transitions
- Any specific actions which they propose to mitigate risks to CORU ICT service provision during the transitions

5.1.3 Transition Management & Staffing

CORU will establish a project board to oversee the implementation of the managed service transition. The service provider will be invited to provide suitably experienced expertise to participate on this board. CORU will appoint a project manager who will oversee the implementation of the service.

The selected service provider will be expected to nominate a project manager who will manage the service provider's resources on the project and assist the CORU Project Manager. The role of the service provider's project manager will be:

- Plan in detail all aspects of the service involving the selected provider and CORU's resources and the existing service vendor.
- Work with CORU Project Manager and, if required, the incumbent, to implement overall service plan.
- Assign tasks to team members and ensure they are carried out on time.
- Ensure deliverables are delivered on time.
- Ensure timely communications
- Manage project risks and issues.

- Report to the CORU Project Manager on project performance and escalate appropriate issues.

Following the transition period, the service provider will be required to undertake the operation of the services. It will be the responsibility of the service provider to ensure that the necessary experience and expertise is available and deployed during the transition to develop and operate the service as provided for.

CORU recognises that it will need to give the service provider access to CORU ICT Resources and current incumbent service providers during the transition phases and it will ensure that such personnel are made available for this purpose.

While existing service provider personnel will be available to participate in transition activities, the new service provider must appreciate that the existing service provider's primary responsibility during the transition period will be the delivery of the current range of managed ICT support services to existing service levels. Consequently, they may not always be available when required. Those Service providers responding to this tender must confirm that they understand and will work within this limitation.

As part of their Tenders, the service provider will need to specify the requirements in terms of their required access to both CORU and existing service provider personnel.

5.1.4 Service Handover & Contract Termination

The selected service providers must confirm they will fulfil handover/exit obligations on termination of any contract awarded as a result of this procurement.

The selected service providers must outline their approach to handover/exit services, this should include the provision of an indicative exit management plan identifying all the major activities they would need to undertake on termination of any contract awarded as a result of this procurement. Additional resource requirements, if any, should also be identified. Tenderers should note and confirm that rates in operation at the commencement of any exit service will apply throughout the exit phase.

On termination of any contract awarded as a result of this procurement, the service provider must:

- Produce a detailed exit management plan as part of this tender response and review and update regularly thereafter.
 - The exit management plan must identify all information needed to allow for the provision of the contracted services by a replacement supplier
- Provide all reasonable assistance to CORU to facilitate the transfer of the contracted services to a replacement supplier.
- Facilitate and co-operate with the transition arrangements of any replacement supplier including the facilitation of the replacement supplier's "due diligence", this includes permitting the replacement supplier to inspect processes of the supplier selected as a result of this procurement to the extent that such an inspection is necessary to adequately explain the manner in which the services are provided.
- Make all documentation produced and maintained during the lifetime of the contract awarded as a result of this tender available.

5.1.5 Transition Costs

The selected service providers must fully disclose all costs and any other fees payable by CORU in respect of the Service Transition arrangements, which they propose to put in place. These costs should be detailed in the Costs Template.

6 Technical Service Requirements

This section details the service requirements from a technical perspective required of the selected service provider.

For each of the technical requirements listed below responses should address, where appropriate, requirements under the headings of:

- Administration
- Security
- Monitoring
- Maintenance
- Technical Support
- Disaster Recovery

Responses should confirm that the Provider has the technical competencies to successfully undertake the management of the systems outlined.

Note: Service providers should be aware when replying to the relevant section that responses must be kept to a maximum of 1000 words. Any content in excess of 1000 words will be discarded.

Please also see the section titled Format of Tender Response below.

6.1 Level 2 Service Requirements

For each of the services listed below, bidders should respond with how they propose to deliver services specified. A limit of 1000 words applies.

SYSTEM/SERVICE	6.1 Level 1 and Level 2 Service Requirements	
TYPE	Technical	
DESCRIPTION	See Appendix for quantities of laptops/desktops A programme to update Older HP laptops to Dell machines is under way and scheduled to complete Q4 2026. This should bring us in line for all end points to be running Windows 11. See Appendix below for standard PC configuration. CORU has approximately 100 staff, all of whom have Active Directory user accounts. Our associates have CORU email accounts and AD accounts in the CORU domain. Laptops - All Dell laptops come pre-configured with a CORU image that has all relevant software, however, the dynamic nature of the organisation Phones - CORU have approximately 85 iPhones. All mobile and smart phones are managed by Ninja One and can be locked, wiped or updated by this system. Rare issues that arise will be logged through the Service Desk and basic troubleshooting of issues will be performed there e.g. troubleshooting mail access where the users AD password may have changed or iPhone wiped as a result of users having entered a pin incorrectly and the phone has to have its profile reapplied through Ninja One. If an issue cannot be resolved by the CORU ICT team who will liaise with supplier (currently Three). An internal CORU resource handles escalations. Video Conferencing Other aspects of meeting room environments are the responsibility of site management, including audio visual equipment, where ultimately the supplier is responsible for support. Level 2 support may, from time to time, be asked to facilitate the connectivity of IP enabled technologies acquired independently of the CORU ICT department, such as time and attendance clocks, access controllers or digital signage.	

	Print services are provided by a separate managed service contract.	
CUSTOMER ROLES	CORU ICT Staff perform the following roles – • Licence and software procurement. • Provision of necessary applications & tools required for the resolution of issues under the Providers responsibility. • Provision of adequate PC, server, storage and network infrastructure. • To maintain available contact points for the Service Desk to escalate tickets to Customer's third-party providers. • Assist Managed Service Provider with decision making, when required. • Manage the release and deployment of desktop software.	
3RD PARTY SERVICES	In general, CORU will manage 3 rd party services.	
MANAGED SERVICE ROLES	SDM	Ensure all Level 2 roles are performed on time and to the customer's satisfaction. Manage escalations.
	Level 2	• Deskside assistance of end users where a ticket can be more effectively resolved with physical proximity or where remote intervention is not possible and phone support cannot resolve this matter. • All tickets should be raised with Level 1 and escalated to Level 2 if appropriate. • Support end-user clinics on remote sites on a scheduled regular preapproved basis. • Coordinate onsite services with 3rd parties and escort to correct equipment as necessary. • Provide hands-on and smart-hands support as required. • Refresh laptop and desktop inventory on an on-going basis, building or rebuilding operating systems, software installs and moving user data from old to new machines in an on-going rolling refresh. • Desk Moves and general IT duties such as maintaining orderly IT Workshop and Comms Room environments.

		• Installation, support and testing of software not in the RACI matrix that has been approved by the Customer. • Training of Level 1 resources for products and services defined in the RACI Matrix and compiling KB articles where appropriate. • Documentation and storing of software version in software library (Definitive Media Library). • Stock Management on all sites, tracking PC's and Laptops including annual physical audit of inventory and retrieval of assets as defined in the IT Asset Management process. • Where required to instigate service improvements, training of CORU staff. • Deskside assistance for mobile, smartphone, tablets, Wireless AP's, common-area visual displays and MiFi issues that cannot be resolved remotely. • Work with the Managed Print Service provider to resolve all printing issues. • Participate in project activities as planned and agreed between Contractor and Customer. • On-boarding and off-boarding of user e.g. delivering brief induction and presentation of IT equipment to starters, collection of IT equipment including phone as part of off-boarding process. • Deploy new desktop software and updated versions of desktop software via SCCM, MEM, group policy, endpoint security console, or any new management tool adopted by CORU during the term of the contract.
	Level 3	• Knowledge sharing and mentoring of Level 1 & 2 to improve the overall service and first-call resolution rates. • Maintaining SCCM in an up-to-date state. • Annual update of base build configuration within SCCM. • Design and creation of new configurations for new builds within

		SCCM as require. (No more than one new build per year). • Create and maintain a security policy for Windows 10, ensuring the client is secured from unauthorized access. • Contribute to the realisation of the strategy of co-management of clients via SCCM and Intune/Microsoft Endpoint Manager (MEM) by carrying out integration activities upon request. • Deliver Windows Feature Update projects to CORU standards and in compliance with CORU policies. Note that it is expected that feature updates will be deployed as in-place upgrades. Such projects may comprise: hardware/software compatibility analysis, remediation of hardware/software compatibilities identified, end-user testing and/or pilot testing before general deployment. While the managed service partner will be expected to project manage the delivery of feature updates, a CORU project manager will also be assigned to monitor the project and provide support for the project. There will be joint ownership of issues, with issues that cannot be resolved by the managed service being escalated to the CORU project manager for resolution or work-around. All relevant configuration documentation will be updated as a part of feature updated. If required, hardware compatibility remediation will be carried out as a part of the PC replacement programme. The frequency of feature update deployments is subject to Microsoft's policy on end of support for Windows builds; however, a 24-month update frequency is planned currently. There will be a compliance target of 90% of in use client devices. • Contribute to design of end user device management architectures and standards.
--	--	---

6.1.1 Level 3 Service Requirements

For each of the services listed below, bidders should respond with how they propose to deliver services specified. A word limit of 1000 words will apply.

6.1.2 Level 3 Services - Active Directory Management

SYSTEM/SERVICE	6.2.1 Active Directory	
TYPE	Technical	
DESCRIPTION	CORU have a robust Network layout across 2 locations • Live (located in the Revenue DC) • Backup (Located in Smithfield Office) As part of the live site, we have 2 domain controllers (Server 2022) and all other VM's. These then replicate overnight to the Backup site. Hardware is mirrored across the two sites, with the addition in Smithfield, of Veeam Backup System on physical and virtual machines.	
CUSTOMER ROLES	CORU Digital and Quality Systems Department Staff perform the following roles – • Microsoft licence procurement. • Procurement of adequate server, storage and network infrastructure. • Governance of accounts – approvals & denials of request for creation/modification/deletion. • Assist Managed Service Provider with decision making, when required.	
3 RD PARTY SERVICES	None	
MANAGED SERVICE ROLES	SDM	Ensure all Level 1,2 & 3 roles are performed on time and to the customer's satisfaction. Manage escalations.
	Level 1	Ticket handling.
	Level 2	Ticket handling.
	Level 3	Full day-to-day management of the AD environment, including but not limited to:
		Administration ▪ Manage Organizational Units (OUs), group policies and logon scripts ▪ Manage the health of the AD database, replication and distributed file system (DFS)

		▪ Modify AD system parameters as required to meet changing business needs or to resolve issues arising ▪ Manage the AD IP Network, sites, and services ▪ Implement appropriate automation and scheduling of administration tasks to improve service reliability ▪ Update and maintain documentation relating to AD configuration <u>Security</u> ▪ Manage the creation and maintenance of AD user accounts and groups. User accounts are created as per CORU process. ▪ Ensure disused accounts are disabled/de-activated as per CORU requirement. Note: Active directory accounts are managed monthly by way of ADManager reporting. ▪ Implement day-to-day security management including security group membership, password policy, event logs and auditing and server compliance. ▪ Review the latest security updates and make appropriate recommendations including testing and deploying patches as per Customer Advisories. ▪ Resolve any issues raised in security reviews. ▪ Ensure appropriate audit logging levels are in use to provide adequate tracking, troubleshooting and review facilities.
--	--	--

		- Manage Account review process to ensure accounts have appropriate privilege and are closed in a timely manner. <u>Monitoring</u> - Ensure optimal replication topology for Active Directory - Pro-actively monitor, pre-empt, diagnose and rectify AD related problems. - Review latest software and security updates and make appropriate recommendations. <u>Maintenance</u> - Implement approved software updates & security patches as per CORU Advisories. - Oversee daily operation of Backups and recovery of individual Servers, databases and Active Directory along with required data. - Carry out testing of new patches, service packs or fixes before deploying to the live environment. <u>Support</u> - Resolve all incidents relating to Active Directory. - Liaise with both Customer teams and suppliers (Equipment & Third Party Software support) to investigate and resolve AD incidents. - Modify system parameters as required to resolve incidents. - Comply with service desk processes and work to resolve incidents within existing service level agreements. - Assistance with the implementation of new projects and initiatives as agreed between Customer and Contractor.
--	--	---

		▪ In the event of an identified security incident on the Supported System, follow the agreed incident escalation procedure. <u>Disaster Recovery</u> ▪ Execute disaster recovery strategy during Customer's DR testing, as required. ▪ Update existing disaster review strategy in accordance with Customer's Business Continuity programme as it matures. ▪ Make recommendations for improvement to AD disaster recovery processes.
--	--	--

6.1.3 Level 3 Services – Exchange/Microsoft 365 Management

SYSTEM/SERVICE	6.2.2 Exchange Management	
TYPE	Technical	
DESCRIPTION	Hybrid O365. Outlook 365 Classic client will remain in use.	
CUSTOMER ROLES	CORU ICT Staff perform the following roles – • Authorising mailbox expansion and enforcing of mailbox clean-up in the event of exceeding the maximum limits • Procurement and provision of licenses • Provision of adequate server, storage and network infrastructure. • Assist Managed Service Provider with decision making, when required.	
3 RD PARTY SERVICES	Tennant Licensing handled by MicroMail.	
MANAGED SERVICE ROLES	SDM	Ensure all roles are performed on time and to the customer's satisfaction. Manage escalations.
	Level 1	Ticket handling.
	Level 2	Ticket handling.
	Level 3	Full day-to-day management of the Exchange environment, both on-prem and in O365, and incorporating management of the Azure AD Sync, Multifactor Authentication and other components of Microsoft365 that may be introduced during the lifetime of the contract, including but not limited to – • Configuration of Exchange components - Outlook clients, Exchange servers, databases, Hybrid servers. • Manage mailbox rights, restoration of mailboxes and security. • Manage the creation and maintenance of user accounts and groups. • Manage shared mailboxes, public folders, rooms, calendars and mail distribution groups. • Provision of standard mailbox sizes with extensions on demand. Currently on-prem there are 6 mailbox sizes and users must request to have a mailbox extended from one to the next. • Implement appropriate automation and scheduling of administration tasks to improve service reliability. • Update and maintain documentation relating to Exchange configuration.

		• Monitoring of critical components • Maintenance of security certificates • Manage the allocation of access rights. • Review latest software and security updates, including notifications from Microsoft relating to O365 and make appropriate recommendations including testing and deploying patches as per Vendor Customer Advisories, testing new patches, service packs or fixes before deploying to the live environment. • Resolve any issues raised in security reviews. • Undertake performance monitoring and tuning and make recommendations for service improvement. • Perform Backups and recovery of individual Servers and Exchange along with required data and ensure correct completion of data backups. • Monitor both internal and external mail queues. • Pro-actively monitor, pre-empt, diagnose and rectify Exchange server and mailflow related problems. • Support, maintenance and troubleshooting of the Exchange infrastructure, both on-prem and in O365. • Resolve all incidents relating to Exchange through service desk processes. • Liaise with both Internal Support Teams and suppliers (Equipment & Third Party Software support) to investigate & resolve Exchange incidents. There are dependencies on Exchange throughout the organisation, e.g. Integra, CRM/CBM, which are business critical. Supported eMail client protocols are native Outlook (MAPI), IMAP4 and OWA (HTTPS). • Assistance with the implementation of new projects and initiatives by agreement between Customer and service provider. • Execute disaster recovery strategy during Customer's DR testing. • Update existing disaster review strategy and in accordance with Customer's Business Continuity plans.
--	--	---

		• Make recommendations for improvement to Exchange disaster recovery processes.
--	--	---

6.1.4 Level 3 Services - Server and Storage Management

SYSTEM/SERVICE	6.2.3 Server and Storage Management	
TYPE	Technical	
DESCRIPTION	(See Hardware and Server Spreadsheet in Appendix A).	
CUSTOMER ROLES	CORU ICT Staff perform the following roles – • Licence procurement. • Provide remote access to servers through use of Team Viewer - and other remote access tools. • Provision of specifications & infrastructure requirements for new application requests or application change requests. • Provision of adequate server, storage and network infrastructure. • Assist Managed Service Provider with decision making, when required (ICT Manager).	
3 RD PARTY SERVICES	All SAN's and servers have vendor support for escalation of issues. Vendor support in place with VMware for escalation of issues.	
MANAGED SERVICE ROLES	SDM	Ensure all roles are performed on time and to the customer's satisfaction. Manage escalations.
	Level 1	Ticket handling.
	Level 2	Ticket handling. Smart hands-on servers.
	Level 3	This service will provide full server operating system management and support, comprehensive server administration and management including on-going monitoring and support. Windows Server is running on Servers in the Staff, Web and Student domains. Ninja One will be used to monitor and push then required the Server patching. The service provider will have and will manage access to the patching without such updates.

		<u>Administration</u> • Manage the install, configuration and management of TCP/IP, DNS and DHCP. • Manage local group memberships on files and folders within file, print and application servers • Install and maintain existing print servers and queues in conjunction with the Managed Print Service. • Implement appropriate automation and scheduling of administration tasks to improve service reliability. • Update and maintain documentation relating to server administration. • Manage Terminal Services and remote access to servers. <u>Security</u> • Ensure that users are assigned the appropriate permissions when requesting access to files & folders. • Review the latest security updates and make appropriate recommendations including testing and deploying patches as per Customer Advisories. • Resolve any issues raised in security reviews. • Access control including the management of file, group and share permissions. • The management of anti-virus applications on Windows servers including proactive identification of virus threats and remedial action in the event of a virus infection.
--	--	--

		• Create and maintain a security policy for Windows servers, ensuring the server and data is secured from unauthorized access. • Ensure appropriate audit logging levels are in use to provide adequate tracking, troubleshooting and review facilities. <u>Monitoring</u> • Monitor the performance of individual servers and make proposals for improvement where appropriate. • Continue use of appropriate server management tools to monitor the availability of services such as file and print, e-mail, internet. (primarily SCOM) • Ensure correct completion of data backups. • Review latest software updates and make appropriate recommendations. • Monitor access to servers and ensure compliance with license agreements. • Make appropriate use of server tools to monitoring security-related events. • Make recommendations in relation to capacity to ensure that current trends and future projects do not lead to capacity or performance issues. <u>Maintenance</u> • Installation of all Service Packs and all recommended software hot-fixes and security updates on all Windows Servers as per vendor advisories.
--	--	---

		• Carry out testing of new patches, service packs or fixes before deploying to the live environment where a UAT or secondary system exists. • Perform Backups and recovery of individual Servers along with required data. <u>Support</u> • Resolve all incidents relating to Windows Servers. • Liaise with both Customer Support Teams and suppliers (Equipment & Third Party Software support) to investigate & resolve Windows Server incidents. • All servers are covered under hardware warranty and the Contractor is expected to process warranty requests. • Comply with service desk processes and work to resolve incidents within service levels. • Assistance with the implementation of new projects and initiatives as agreed between Customer and Contractor. • In the event of an identified security incident on the Supported System, follow the CORU incident escalation procedure. <u>Disaster Recovery</u> • Execute disaster recovery strategy during Customer's DR testing. • Update existing disaster review strategy and in accordance with
--	--	--

		Customer's Business Continuity programme. • Make recommendations for improvement to Server disaster recovery processes. <u>Remote Offices</u> • The Contractor will manage and maintain servers in remote offices. <u>Server Builds (Builds Management)</u> • In the event of a service failure, the Contractor will re-build servers to Operating System level and then fully restore data and supported applications. • The Contractor will coordinate the server to be shipped at the Customer's expense to the relevant location and made operational. <u>Server Failure</u> • In the event of a server failure, where the server needs to be replaced, the Contractor will rebuild the replacement server using the appropriate Windows Server builds. • The Contractor will coordinate the server to be shipped at the Customer's expense to the relevant location and made operational. <u>Anti-Virus Management</u> • Proactive identification of virus threats and counter measures.
--	--	--

		• The management of anti-virus applications on Windows servers and desktops. • Ensure the continual updating (automatic) of the antivirus products with the latest virus signature definitions as soon as they become available from the application providers. • Taking any remedial action necessary in the event of a virus infection. • The CORU ICT Security team will retain access to all anti-virus servers and tools for reporting and service provider compliance auditing purposes. <u>Web Services</u> • Support of basic IIS (Internet Information Server) software • User permissions allocations • Locked and restricted authentication options for intranet pages (network user-ID & password) – intranet sites only • Support of industry standard certificates for web sites – installation & maintenance • Monitoring of web service availability <u>Documentation</u> • Maintain build documentation
--	--	---

6.1.5 Level 3 Services - Backup Management

SYSTEM/SERVICE	6.2.9 Backup and Restore	
TYPE	Technical	
DESCRIPTION	As all servers are VM clients in a VMware vSphere v8 the backups are handled using Veeam Backup & Replication v13	
CUSTOMER ROLES	CORU ICT Staff perform the following roles – Monitor emails for any error reports, provide level 1 support on reports and if needed escalate to 3rd Vendor.	
3 RD PARTY SERVICES	A Maintenance & Support contract, renewed annually with Veeam, includes direct access to their in-house Veeam engineers for technical support.	
MANAGED SERVICE ROLES	SDM	Ensure all Level 3 roles are performed on time and to the customer's satisfaction. Manage escalations.
	Level 1	Ticket handling.
	Level 2	N/A
	Level 3	Full day-to-day management of the Veeam backup environment, including but not limited to: - Configuration of Veeam components - clients, backup agents, storage policies, media agents, schedules, etc. - Monitoring, morning checks, same-day troubleshooting of failed backups, daily summary report. - Completion of restore jobs as required. - Manage monthly backup tape changes (tapes changed by Department of Agriculture staff, on instruction). - Deployment of upgrades – Feature Releases and Maintenance Releases – as scheduled by the customer. - Monitoring Veeam generated Health Check reports and resolving Critical issue alerts and SLA alerts. - Perform set of test restores every six months.

6.1.6 Level 3 Services – LAN, Wireless & Firewall Management - List

SYSTEM/SERVICE	6.2.10 LAN, Wireless and Firewall Management -	
TYPE	Technical	
DESCRIPTION	See Network Inventory in Appendix A for full inventory. WAN links There are WAN links in 2 Data Centres. All CORU Campus sites have a 1 Gb link on Government Cloud Network (GCN). GCN is a high-speed network designed to connect government agencies together to use a shared infrastructure. Backup links are configured with automatic failover. The WAN links and associated switches and routers are managed and monitored by the Network Providers. CORU also monitor availability and performance of the WAN links and provide smart-hands when necessary for the CPE devices. Data Centres Most IT Services are based in the Revenue Data Centre (DC1) – e.g. Business applications, DMS, Exchange, file and print services. Both of CORU Data Centres DC1 & DC2 have 10Gb switches for LAN and SAN and 1Gb switches for physical servers and DRAC connections and are linked over Government Networks and internet are provided by Government Networks. Government Multi Media VLAN is used for VoIP. Smithfield Data Centre (DC2) is the backup and replication site and Failover should there be an issue at DC1. Firewalls For perimeter security, FortiGate 200F firewalls are used. VPN access is handled by the 2 FortiGate 200F firewalls (in RDC) with authentication handled by FortiAuthenticator. Site to Site VPNs on the FortiGate firewalls are used for Business Partner and some Cloud Services. Troubleshooting users VPN connections to CORU is within scope of Managed Services, while users home broadband connections are not within scope, although advice may be given to users. LAN switches 12 Switches – all Cisco – not under management.	

	It is expected that improvements to security of the LAN will be carried out during the lifetime of the contract. Configurations for all network devices should be backed up weekly by MSP. All WAN, LAN and other network related devices are monitored MSP Wireless CORU use Fortinet cloud to manage all AP's in Smithfield.	
CUSTOMER ROLES	CORU ICT Staff perform the following roles – • License procurement. • Upgrade policy and scheduling of upgrades. • Provision of adequate server, storage and network infrastructure. • Provision of cabling services for connecting new points • Assist Managed Service Provider with decision making, when required (ICT Manager).	
3RD PARTY SERVICES	Manufacturer support services. WAN links and associated Customer Premises Equipment are configured and maintained by the providers, in conjunctions with CORU and the Managed Service.	
MANAGED SERVICE ROLES	SDM	Ensure all Level 3 roles are performed on time and to the customer's satisfaction. Manage escalations.
	Level 1	Ticket handling.
	Level 2	Ticket handling. Smart hands.
	Level 3	<u>Administration</u> ▪ Administration of the LAN, Wireless, Networking, Web Filtering and Firewall environment including managed wireless to include new configurations, rule changes and modification of system parameters to suit user operating environment along with general administration. NOTE, at times it is required to make changes to ASA firewalls and other network devices via CLI to maintain the readability of the configuration. ▪ Update and administration of the Orion network monitoring service.

		▪ Configuration and replacement as necessary, adhering to Customer policies. ▪ Making changes where necessary to provide higher levels of security and service. ▪ Maintaining accurate and up to date documentation to include network LAN and WAN network diagrams, spreadsheet information on IP addressing, WAN links, network switches, Wireless APs. <u>Security</u> ▪ Manage the allocation of access rights. ▪ Review the latest security updates and make appropriate recommendations including testing and deploying patches as per Customer Advisories. ▪ Be alert to and make recommendations to improve security e.g. ACL, VPN parameters, SNMP version, SSH version ▪ Resolve any issues raised in security reviews. <u>Monitoring</u> ▪ Proactive monitoring of the LAN Network and Firewall environment including system performance, reliability and capacity planning. ▪ Report on performance issues and make recommendations to improve performance including working with CORU and suppliers to determine best solution, testing and deploying updates or configuration changes <u>Maintenance</u> ▪ Firmware and OS Upgrades in keeping with vendor recommendations and CORU own schedule of patch and vulnerability programme.
--	--	--

		▪ Carry out testing of upgrades or fixes before deploying to the live environment. ▪ Upgrade of Orion Solarwinds on a regular basis <u>Support</u> ▪ Resolve all incidents relating to Networking. ▪ Troubleshoot and fully manage support incidents. ▪ Testing the backup and recovery procedures on a regular basis. ▪ Testing failover of WAN links on a regular basis, and measuring bandwidth on the primary and backup links <u>Disaster Recovery</u> ▪ Weekly backup of all switch, firewall, SBC, Netscaler, Wireless configurations. This must be saved on the File server so it can be included in the Veeam Backups. ▪ Aid in the monthly, Quarterly and yearly DR schedule as laid out in the DR Policy. Restoration and recovery of service in the event of Switch failure. ▪ Make recommendations for improvement to recovery processes. Assistance with the implementation of new projects and initiatives by agreement between Customer and Service Provider. It is expected that the Service Provider will provide expert advice on CORU network related issues or projects and will design solutions and/or assist in designing solutions.
--	--	---

6.2.12 Security - List

SYSTEM/SERVICE	6.2.12 Security	
TYPE	Technical	
DESCRIPTION	The role of Managed Service is in administration and operational tasks and in providing input to decision-making. <u>Tools currently in place are:</u> NinjaOne RMM FortiClient ManageEngine 360 Barracuda message Archive CrowdStrike Falcon Complete	
CUSTOMER ROLES	CORU ICT Staff perform the following roles – • Software and Licence procurement. • Creation and maintenance of Access Control, Security and Data Protection policies • Defining Upgrade policy and scheduling of upgrades with MS provider. • Provision of adequate server, storage and network infrastructure. • Assist Managed Service Provider with decision making, when required (ICT Manager). • Review all user accounts and their privileges regularly. • Defining future requirements • Agreeing processes and procedures with Managed service providers.	
3 RD PARTY SERVICES	All tools in use have vendor warranty and support contracts in place.	
MANAGED SERVICE ROLES	SDM	Ensure all Level 3 roles are performed on time and to the customer's satisfaction. Manage escalations.
	Level 1	Ticket handling.
	Level 2	Ticket handling.
	Level 3	• The Managed Service provider will administer and maintain the associated systems. • The Managed Service provider will handle incidents through the agreed

		process to the level defined for hand over to CORU ICT team. • Designated systems used for monitoring and reporting will be configured by the vendor to achieve desired levels of reporting. • The Managed Service provider must subscribe to Vendor advisories for all commonly used or critical software and hardware in the environment. (e.g. Dell, VMware, Microsoft, SolarWinds, Cisco, Fortigate), as well as Global alerts relative to the ICT estate, including Mobile operating systems (iOS) • The managed service provider must subscribe to product notifications for zero-day vulnerabilities. • The managed service provider must establish a structured approach to the monitoring of external threats. • The Managed Service provider must schedule patching in accordance with the CORU Patch and Vulnerability Parameters document, the most recent copy of which is provided in Appendix D. • Report on all server and endpoint patching levels through SCCM and remediation of patching issues. • The managed service provider must carry out a quarterly vulnerability review of network hardware [routers, firewalls <i>as an example</i>]. They must advise CORU on vulnerability updates and patches that must be applied. This review must also advise on unused feature sets that should be disabled etc. See Table under Appendix A <u>PKI Certification:</u> • Status Monitoring- Monthly report on certificate status on servers • Certificate Installation onto servers and applications - internal and third-party CA
--	--	--

		• Certificate renewal for internal certificates. • Administer PKI servers to enable certificate-based network authentication. • PKI server infrastructure maintenance • Defining certificate templates • Requesting third party certificates (Creation of CSR for third party certificate/public certification requests) <u>Fortigate Infrastructure:</u> • Patches to be applied as per schedule. • Firmware updates as per schedule. • Report on system status on monthly basis. • Report on user activity on weekly basis. Fortianalyser server and scheduled reporting currently in place. • Release and blocking of URL's and applications, on authorisation or by agreed process. <u>ADManager admin and audit tool</u> • Maintain tools used in AD reporting (ADManager/ADAudit) in conjunction with Security team. • ADManager and audit tool DB's must be maintained. <u>LanSweeper</u> • Maintain and configure LanSweeper plus its DB in conjunction with the Security team. <u>Access Reporting & Monitoring</u> • Live monitoring for unauthorised activity on the network using agreed reporting tools. • Monthly reporting on incidents detected and resolved under agreed process. • Reporting on exceptions issues escalated to CORU teams. <u>Nessus:</u>
--	--	---

		• Maintain and configure Nessus in conjunction with the Security team. <u>Endpoint protection + Drive Encryption:</u> Crowd Strike is the current endpoint protection used and this is bundled with and supported my 3rd Party Vendor Ninja One • Keep all client/server software agents and components up to date. • Keeps all drive encryption software agents and components up to date. • Install endpoint protection client/server software and components onto appropriate systems. • Install drive encryption software and components onto appropriate systems. • Remediate any client/server issues that may arise for either the endpoint protection or BitLocker. ▪ Ensure that 100% of devices defined for encryption are secured and reporting as such. ▪ Policy maintenance and revision. ▪ Reporting and alerting ▪ Proactive identification of virus threats and counter measures. ▪ Taking any remedial action necessary in the event of a virus infection. ▪ Liaise actively with the customer ICT Security specialist to ensure that relevant policies are being enforced. <u>RSA</u> • Administer RSA Secure ID infrastructure. • Maintain server software and patching • Install RSA tokens and seeds • Issue and distribute RSA tokens • Resolve normal issues. • Report on issues escalated to CORU • Manage Tokens - Monitor unused tokens and redistribute <u>Data Protection</u> • Lock users and systems on request from ICT-M
--	--	---

		• Report on activity to ICT-M • Maintain confidentiality in all Data protection cases.
--	--	---

6.2 Additional Expertise

Description

CORU will look to the selected provider to guide them with other resources such as Database Warehousing, Network Architect, SharePoint Administrator, System Automation, AI, Chatbots and Cybersecurity. Also, Active Directory expert for work such as on Group Policy, Office365 Administrator and/or Architect, Project Manager or Security Expert might be called upon for specific pieces of work, if available. A rate card for such resources, from which a resource can be drawn, should be submitted, specifying day-rates for each available skillset.

A piece of work may also be commissioned on a fixed number of such days with the scope of work being defined by agreement between CORU and the Provider before commencement and any variation +/- outside the days agreed being absorbed or retained by the Provider.

A Project Lead Resource Day Rate would also be desirable for inclusion on the Rate Card. A description of the envisioned scope and responsibilities of this role is provided here for clarity.

Project Lead Description of Deliverables

- Provide an onsite or Remote Project Leader or Senior Technical Resource who may double as a Project Lead.
- Project Leader/Resource will use PRINCE2 as base methodology and will own delivery of mini-projects
- Ensure a co-ordinated approach is taken to the delivery of all services including the management of interdependencies and risks.
- Should incidents result in a mini-project to rectify, manage the link between incident and Change Management
- Management of change to the assigned live environments while maintaining the accuracy of associated systems documentation.
- Reporting on project delivery as agreed.
- Provide advice and guidance on any matters relating to the CORU ICT environment.

Project Services

- Change requests and mini/micro-projects not falling into the scope of the Support Services Framework contract and existing Project Queue.
- This priority is variable depending on the business demands.

- A process shall be agreed for the scoping, scaling and sizing of the work request. The individual case-by-case requirements shall be agreed between the Customer and the Contractor, including skill set requirements, effort estimates, potential impacts to services or other changes/micro-projects, and additional costs (if any).

Customer Responsibilities

- Own the processes post agreement
- Jointly participate in initial and on-going development of projects
- Jointly participate in change and project reviews
- Provide advance notice of at least 2 weeks for major change requests or mini projects.

7 Continuous Service Improvement

Prospective Tenderers should note that CORU are seeking a partner that will look to continuously improve the services experienced by the end-users, and they should also ***note the number of marks being awarded to this area.***

Prospective Tenderers must therefore clearly demonstrate how they intend to continuously improve their service offering, preferably using examples of previous continuous improvement mechanisms. For clarity, the terms end-user and Customer are equivalent in this section of the RFT.

Specifically, tenderers must demonstrate:

1. How they will interact with end-users in a proactive manner
2. How they will seek to prevent issues occurring in the first place
3. How they intend to automate routine processes and requests so that end-users see rapid turnaround of issue resolution and service requests
4. How they will seek to promote efficient and effective resolution of tickets raised
5. How they will measure service improvements
6. How they will seek to alter the Culture in CORU so that confidence in a measured service will increase.

Tenderers must outline if and how they will introduce self-service tools, how they will measure the effectiveness of such tools, how they will disseminate learnings from end-user interactions and how they will add to the knowledge of all end-users and technical staff supporting these Customers.

Tenderers must indicate how they will derive a baseline for the value being delivered to end-users and Tenderers must then outline how they will seek to add value to the service delivered, over the lifetime of the service, such value to be measured at the Customer level.

Tenderers must be prepared to estimate targets for value improvement and should be aware that such targets are likely to be included in a Service Level Agreement.

Tenderers must indicate how the Service they offer will become more Agile as the service matures and how they will facilitate Agile delivery of product to the end-user.

Tenderers should be aware that CORU anticipates that staff numbers will increase by up to 25% and registered service providers will increase by up to 50%. It is to be

understood that service levels will not worsen, and ideally should improve, as the organization grows.

8 Format of Tender Response

To aid prospective suppliers in their submissions and to assist CORU in the evaluation process, two Tender Response Documents are included with all relevant requirements and sections for responses to be completed. While CORU has made every effort to ensure that this Response Document is accurate no responsibility shall lie with CORU for any omissions.

Prospective service providers should particularly note the facility in the Checklist Tab of Tender Response to detail the location in their Response to this Tender where responses to specific requirements are listed.

Suppliers should note that failure to supply mandatory information may result in disqualification of their tender, irrespective of total qualifying scores.

CORU require that prospective suppliers provide a response to this tender by submitting a full Tender structured according to the format below:

- a. Checklist For Tender Submissions
- b. General Information
- c. ESPD, Statements & Declarations
- d. Declaration As To Personal Circumstances of Tenderer
- e. Declaration Re Statutory Obligations
- f. Economic & Financial Selection Criteria
- g. Technical & Professional Criteria
- h. Organisation Profile & Background
- i. Award Criteria

9 Cost Requirements

9.1.1 Introduction

Please use the Tender Response Document B spreadsheet to complete Cost Requirements.

CORU requires a fixed price contract for the first two years of this contract and for each subsequent year of the contract. The tenderer is required to provide details of all costs. All costs quoted should be in Euro. Details of VAT and any other taxes or duties that may be incurred should be shown separately.

9.1.2 Managed Services

The tenderer must state the overall costs and provide a detailed breakdown of costs under the following headings:

Part 1 - Transition:

- Tenderers should detail the costs of their transition plan. These will be scored under Section B3.1 and not under scored overall Cost.

Part 2 - Managed ICT Infrastructure Support services

- Level 2 Services
- Level 3 Services
- Active Directory Management Service
- MS Exchange Management Service
- Server and Storage Management
- Backup Management
- LAN, Wireless and Firewall Management
- Security Management
- Addition Expertise
- All other costs

Risk Plan:

- Tenderers should detail the costs of any risks associated with the provision of this service

Part 3 – Additional Expertise

- Tenderers should detail the daily rates for use for Additional Expertise. These will be scored under Section B1.31 and not under scored overall Cost.

9.2 Additional Costs

List separately any additional costs which you foresee and which are not included in the above. No further costs may subsequently be added.

9.3 Completeness of Costs

The tenderer must include all costs under one of the headings in this section. No additional costs may subsequently be introduced. Any costs not included in this section of the tender response will be deemed to have been waived.

10 Compliance Checklist

10.1 Instructions for Tenderers

The *Checklist* tab of the Tender Response Document B spreadsheet provides a checklist to use. The MDI column indicates the importance of each requirement to CORU.

MDI column:

- M: Mandatory. CORU states that this is a mandatory requirement.
- D: Desirable. CORU states that this is a desirable requirement.
- I: Information. This point is for information purposes. Please comment on it.

Tenderers will complete the YNP column in Tender Response Document A as follows:

YNP column:

- Y: Yes. Compliant.
- N: No. Not Compliant.
- P: Partially Compliant.

And further elaboration in the Comments Column.

Responses to these sections is contained, where applicable, in Tender Response Document A and Tender Response Document B.

Note that the responses to these requirements will form part of the contract between CORU and any selected supplier.

Each response on the checklist will be assigned a mark, and these scores will be weighted to arrive at a final score for each tenderer.

11 Appendix A Current Environment

11.1 Comms Room 5th Floor

Switches

- 4 x Cisco 2960X (1 x Government VPN VLAN Switch)
- 1 x Cisco 2960S
- 1 x Cisco 2960G
- 2 x Cisco 3750X
- 2 x Cisco Catalyst 9300- 48
- 2 x DELL EMC S5212F-ON

Firewalls

- 2 x FortiGate 100D

Host Servers

- 2 x Dell PowerEdge R660
- 2 x Dell PowerEdge R760

SAN

- 2 x NetApp hosts

Tape Library/Autoloader

- 1 x Quantum Scalar i3

11.2 Revenue Data Centre

Switches

2 x Cisco Catalyst 9300- 24

Firewalls

2 x FortiGate 200F

Host Servers

2 x DELL EMC S5212F-ON

1 x Dell PowerStore 500T

2 x Dell PowerEdge R660

11.3 Software:

Installed on all laptops

- Office 2016 (32 or 64 bit)
- 3CX Webclinet/Desktop App
- FortiClient VPN Agent (free version)
- Ninja One agent
- Adobe Acrobat / PDF Complete
- TMS Client

CORU Department Specific:

Legal

- Practice Evolve (SaaS)

Registration & Recognition

- Thentia Cloud (SaaS)

Secretariat

- Decision Time Meeting Management (Portal)

Human Resources

- TMS Time Management System

Finance

- Sage (SaaS)
- Payroll

Governance & Compliance

- Decision Time Risk Management

ICT

- Ninja One RMM (SaaS)
- 3CX Administration console
- Exchange Administration
- Active Directory
- VMware vSphere V8
- Veeam backup and Replication 13

11.4 Endpoints:

- Dell Laptops running Windows 11
- End of life HP Laptops running Windows 10 or 11
- Micro PCs running Windows 11

All devices are managed through Ninja One RMM

12 Appendix B RACI

Please see below Current RACI, which is likely to change as the service evolves.

Responsibility Matrix (RACI):

	CORU ICT Team	CORU ICT Manager	MSP Support Representative	MSP Support Manager	Head Corporate Services
Level 1 helpdesk	R	R		I	
Level 2 helpdesk	R	R	R	I	
Level 3 helpdesk		A	R	C	I
Hardware Failure		A	R	A	I
Server Outage		A	R	A	I
Patch Management		A	R	I	
Backups		A	R	I	

13 Appendix C ICT List of current ongoing projects

Yet to commence:

- Implementation of a Quality Management System
- Data Warehousing development
- Automation and AI implementation

Live Projects

- Registration Management System Development and Procurement Support
- TMS required upgrade and migration to SaaS (Ongoing)

14 Appendix D CORU Standard Terms and Conditions

Insert

15 Appendix E – CORU Digital Strategy Strategy

[add]