ICT Managed Services

Statement of Work

07/06/19

Table of Contents

Introduction

The Royal Dublin Society (RDS) is Ireland's leading philanthropic society. It's Foundation Work Programme spans across science, the arts, agriculture, enterprise and equestrianism, and is funded by the commercial operations located in the RDS venue as well as philanthropic donations. The RDS is a registered charity. The purpose of all commercial activities is to ensure the continued delivery of its Foundation mission.

The venue is a 40-acre campus with a mixture of facilities which hosts a wide range of events. In 2018, the RDS will host circa 320 commercial events attracting circa 1.8m visitors to the campus. In addition, the RDS will host hundreds of Foundation events. The success of the RDS, given the complexity of the event calendar in terms of both the scale and variety of events, is due to a number of key strengths including:

- The venue location
- The longstanding relationships with the clients
- The flexibility of the venue to become whatever the client desires
- The flexibility of staff and the RDS service offering

The venue is supported by a complex architecture of applications and infrastructure supporting both the commercial and Foundation activities of the RDS.

.
The RDS now wishes to engage an external supplier to provide IT Managed Infrastructure, Backup and DR services for the RDS Administrative Offices. The RDS Administrative office IT environment is a virtualized solution which includes a fully redundant virtual private cloud infrastructure based on VMware vSphere 6.5 technology (35 servers) with NetApp SAN and a Virtual Desktop environment on the VMWare Horizon 7 platform (90 desktops) with Windows 7 as the standardized operating system.

RDS is looking for a solution that:

- is easy to manage both commercially and operationally. From a commercial perspective this means providing RDS with predictable upfront pricing which allows accurate budgeting over the term of the Contract. From an operational perspective this means providing a single point of contact for all of RDS's IT requirements and managed third party providers.
- delivers requirements quickly and efficiently. Current and future requirements must be implemented within the timescales set out by RDS, with minimal disruption to RDS's operating environment, and together with all necessary processes, documentation and training.
- are flexible with respect to future requirements and service options. RDS must not be limited in respect of additions or amendments to the solution and RDS must not be tied to any particular support provider except as provided in the contract.
- is cost-effective both at the start of the Contract and as the service grows.

Scope Overview

The services within the scope of this tender are given in the table below

Service Item	In Scope
Managed ICT Infrastructure	
Server and Storage monitoring (physical and VM)	***Included***
Systems Software Support (Windows Server, Active Directory, VMWare, Veeam)	***Included***
Database Support (SQLServer)	***Excluded***
Desktop/Laptop management and monitoring	***Included***
Servers - Break/fix	***Included***
Storage - Break/fix-	***Included***
Laptop/Desktop - Break/fix	***Included***
LAN support - Including Break/Fix	***Excluded***
WIFI Support - Including Break/Fix	***Excluded***
WAN Support - Including Break/Fix	***Excluded***
Mobile Phones	***Excluded***
Anti-Virus/Ransomware Software Support	***Included***
Managed Firewall (including Intrusion Detection and Prevention)	***Excluded***
E-mail filtering	***Excluded***
Server Patching	***Included***
Out of Hours Cover – Remote	***Included***
Out of Hours Cover - On-Site	***Included***
Out of Hours Cover - Server Monitoring	***Included***
Office 365 Provision and Support	***Included***
Virtual Desktop Support	***Included***
Firmware Upgrades	***Excluded***
Application Support	***Excluded***
Asset Management	***Included***
Software License Management	***Included***
Third Party Vendor Management	***Included***
Security Assessment (Including penetration testing)	***Included***
Professional/Project Based Services	***Included***
Disaster Recovery as a Service	***Included***
Backup as a Service	***Included***
Security as a Service	***Included***

The scope of the environment to be managed by the successful tenderer is outlined in Annex 1.

It is anticipated that one service provider will be appointed. However, the RDS may, at its own discretion and to ensure acceptable performance and cost, appoint a second provider for some of the services and / or related projects.

The service contract will be subject to annual review and satisfactory performance.

The RDS requires tenderers to nominate an Account manager who will act as the main point of contact for the duration of the contract. This person shall have the authority to deal with all matters in relation to the contract and be responsible for the satisfactory delivery of the services required. The duties of the account manager will include the following:

a) Overall responsibility for a good working relationship with the RDS;
b) Meet as and when required to review the relationship and examine performance;
c) Deal with disputes, complaints or concerns that cannot be adequately resolved;
d) Regularly give and receive both formal and informal feedback on the relationship, workloads, processes, areas and suggestions for improvement and cost savings;
e) Proactively discuss with the RDS of improving efficiency regarding service delivery in general.

Managed IT Infrastructure

The following ITIL services are considered in scope for the covered infrastructure:

a) Availability management
b) Service level management
c) Capacity Management
d) Change management
e) Release and Deployment Management
f) Service asset and configuration management
a) Event management
b) Incident Management
c) Problem Management

The RDS requires the vendor to provide the following:

a) Provide a remote ICT helpdesk support service to log calls via phone, e-mail or web portal, track and escalate calls as required
b) Provide remote first and second level call resolution services for incident and problem management
c) Provide proactive monitoring and remote alert monitoring service for critical infrastructure and take appropriate, agreed actions to prevent and eliminate any service outages for the following:
    - physical hardware (compute, storage)
    - Virtualized servers and desktops
    - System software (virtualization, operating system, database other)
d) Provide software solution support:
    - Microsoft Windows (desktop and server) and Office
    - Sophos
    - Veeam backup and restore
    - VMWare
e) escalation and workflow activities associated with managing a helpdesk service.

f) Provide daily monitoring reports indicating status of critical infrastructure

g) Provide monthly service and trending reports on KPI's, detailing the monthly service activities, call patterns, trends and identifying areas for service improvement.

h) Provide timely patch management services for the RDS servers in the virtualized environment (both production and DR).

i) ensure that information regarding technical vulnerabilities is obtained in a timely manner, evaluated for its relevance and potential impact to the organization's assets, and appropriate measures taken to address the associated risk.

j) Provide support and maintenance of the desktop and laptop environment and ensure all updates (including Anti-virus) are applied

k) Provide on-site service to carry out fixes and remedial work which cannot be performed remotely

    - Break/fix support including hardware repair and replacement including Liaison with vendors when equipment is still under warranty
    - Server, PC and Laptop repair

l) Provide 3rd party management services to manage RDS 3rd party service providers where required. For example:

    - Firewall/network service providers
    - Print Management Solution providers

m) Provide an emergency call out service to respond to urgent out of hours incidents on a 24X7 basis at certain times during the year (due to the nature of RDS's business this support may be required during statutory holiday periods)

n) Quarterly heath checks and Preventative maintenance

o) Monitoring of Capacity on storage and compute devices and alerts if specified thresholds have been reached

p) Maintain configuration details for all in-scope equipment

q) Performance and capacity management

    - Monitoring of server capacity, backups, server down/reboot activity, CPU/memory threshold alerts

A RACI table for each of the ITIL Process is given in an appendix.

A full list of infrastructures to be covered under the managed IT Infrastructure services is given as an annex.

The vendors providing the service will establish their service such that they can meet or exceed the following service levels:

Service Element	Performance Required
Service Desk Hours of Operation – including Deskside Support remote support	Standard Services 07.30am – 6pm Monday to Friday
Service Desk Availability	99.95%
Managed Infrastructure operating hours	24/7/365
On-Site Support	Standard Services 09.00am – 17.30pm Monday to Friday 24X7 during defined periods during the year
Scheduled Technical Support	On-site as needed
Response Times • Severity 1 Definition - All users on a site unable to work. Example: Network failure, Server crash, Email server failure, Virus Outbreak • Severity 2 Definition -A group of users unable to work or all users greatly inconvenienced. Example: Single virus, Users machine crashed, Internet outage, Important File unavailable, • Severity 3 Definition - General question, enquiry or problem that does not affect any user's ability to work. Example: I am locked out of my pc/laptop, can you change my password? my Citrix session is hanging, can you close my session?	Severity 1 - 15 Minutes Severity 2 - 2 Hours Severity 3 - 8 Hours
Resolution Times	Severity 1 – 2 Hours Severity 2 - 8 Hours Severity 3 - 24 Hours

While there is no requirement for a 24/7/365 service desk, there is a need to provide on call emergency service desk support outside the standard hours of operation. Service providers should indicate their capability to deliver such an on-call emergency service on a 24X& basis at key periods during the year (for example during the Horseshow 24X7 support will be required) and detail the mechanism they propose to deliver the service.
The RDS will provide remote access to all infrastructure to allow the service provider to provide real-time and pro-active monitoring /support.

The above requirements will be the subject of a Service Level Agreement as defined in schedule 2 which will include an element of fees at risks in the event that Service Levels are not met.

Back Up as a Services

The Service Provider will be responsible for managing and supporting the RDS's existing storage and backup infrastructure including managing all relevant. The services required by RDS include (but not limited to) the following:

a) Provision of cloud-based backup storage

b) Daily on-site backup monitoring

c) Daily off-site backup monitoring

d) Monthly storage usage health check

e) Capacity planning

f) Successful and failed backup history

g) Ticket history

h) Regular back-up testing and file retrieval.

The existing backup schedule is provided as an annex.

Disaster Recovery as a Services

The vendor must provide and support a cloud-based disaster recovery solution. The DR solution should be developed in such a way as to ensure recovery of critical infrastructure which should meet or exceed the following:

- Recovery Time Objective - 2 Hours
- Recovery Point Objective – 2 Hours

The services required by RDS include (but not limited to) the following:

a) On-demand DR infrastructure to support critical servers when needed

b) On-demand DR infrastructure to support virtual desktops when needed (currently based on Windows Remote Desktop)

c) On-going monitoring of data replication to support DR

d) Provision of support services to ensure recovery when the RDS disaster recovery plan is invoked

e) Disaster recovery testing on a regular basis (at least once every 6 months) with a documented report on the outcome of the test

Security Services

The vendor will be required to provide, on an annual basis a security assessment (including vulnerability and penetration testing) of the RDS's ICT infrastructure. The RDS may also require additional penetration testing on an as needed basis after major upgrades

The services required by RDS include (but are not limited to) the following:

f) Controlled external and internal penetration testing directed at perimeter security, including internet firewalls, routers, switches, web servers, application servers, database servers, gateways and security management systems (i.e. AV software)

g) Port scanning and mapping internal and external interfaces.

h) Vulnerability scans to proactively test the Infrastructure for known weaknesses, which could potentially be exploited maliciously

i) Website/web application portal assessment (SQL Injection, ·Broken Authentication and Session Management)

j) Password cracking – Attempting to guess passwords using password cracking tools

k) Server assessment (System & OS Fingerprinting, OS security configuration. Assessment of OS Hardening)

l) Spoofing - assess the scope of potential spoofing attacks i.e., IP, ARP etc.

m) Lockout Testing: To mitigate the brute force attack

n) Physical security assessment of the environment

A documented report should be produced which details know vulnerabilities and suggested remedial action.
The report should include:

o) An executive summary

p) A description of the assessment and the testing which was carried out

q) An overall assessment of security measures

r) Documentation of key security vulnerabilities which have been identified

s) Proposed Remedial actions to address the security vulnerabilities

Implementation of any remedial action is not within the scope of this RFT

Professional/Project Services

The RDS has a requirement to manage and deliver change projects (infrastructure upgrades etc.)in the current and future ICT environments. RDS will require its selected service provider to provide support for these changes.

The services required by RDS include (but are not limited to) the following:

a) Act as ICT partner and providing advice on equipment and systems software selection

b) Carry out an annual review of the ICT environment with recommendations for improvements and upgrades

c) Provide ad-hoc and project support for ICT projects including the replacement of existing infrastructure and the implementation of new technology

d) provide planning services and must assist and support in developing and updating the long-range, comprehensive plan for the RDS's infrastructure, telecommunications services systems, processes, technical architecture and standards.

e) proactively identify strategies and approaches for future service delivery that the vendor believes will provide RDS with increased efficiency, effectiveness, performance, or cost savings.

Project services and advisory services will be based on a man days basis or a fixed price fixed scope as agreed between the parties.

It is estimated that there will be at least 25 professional service days required per annum, but this may change depending on what ICT projects are approved.

Additional Services

As part of the tender response The RDS would welcome proposals from vendors in relation to projects which have the potential to improve the infrastructure and which would reduce complexity leading to a more reliable and robust services for users. For example:

- the NetApp SAN is approaching end of life and RDS would expect to replace it during 2020
- Options on continuation of use of the virtual desktop infrastructure or replacement with an alternative solution

The vendor is free to propose other projects which have potential benefit.

Vendor Response Requirements

The following sections outline the information that is required from the Service Provider in order to evaluate their response to the tender. Please note that the responses should be concise. Off the shelf material can be provided as an appendix.

The response requirements are broken into the following sections:

a) Vendor Contact Details
b) Vendor Company Details
c) Service Scope
    - Managed IT Infrastructure
    - Disaster Recovery
    - Backup
    - Security
    - Professional Services
d) Transition Plan
e) References
f) Cost – There is a separate Excel cost matrix.

Contact Details

Information Requested	Response
Name	
Title	
Address and Location	
Telephone No	
E-Mail Address	

Vendor Details

The following information should be provided

Information Requested	Response
Provide a brief outline of the history and background of the company, including corporate strategy, no. of years in the business, number of employees, etc.	
Outline where the company's support operation is located and where support engineers dispatched from?	
Identify and discuss any major business and technology partners (hardware, software and systems integrators) with which your company has aligned itself Please note that RDS requires proof of a partnership with Microsoft (Azure, O365), NetApp, Sophos, Veeam or Vmware. Alternatively, where such partnerships are not in place the RDS will accept a back to back service agreement with a party who has such agreements in place. However, the vendor remains responsible for service provision and must manage the relationship with the 3rd party.	
Provide a high-level organizational overview of your Company	
Provide details of ISO27001 Certification	
Confirmation that Insurance cover in place meets the RDS requirements as specified in the RDS standard supplier framework agreement. Please note that the RDS will look for confirmation of insurance cover prior to contract signature.	
Confirmation that the vendor is prepared to accept the RDS standard supplier framework agreement. Any exceptions should be clearly stated	
Provide details of any sub-contractors which will be used in the delivery of the	

Information Requested	Response
services. This should include cloud-based providers. Where cloud-based providers are used please indicate that their data centres are based in the EU and are GDPR compliant as well as certified to ISO27001	

Service Scope

Managed ICT Infrastructure

Information Requested	Response
Provide a description of the solution which is proposed for the RDS focusing on key services	
Please provide details of your proposed service delivery process, detailing your process for call logging, processing, escalation, resolving and root cause analysis.	
Provide details on what software tools will be used to provide the service and what impact this will have on the RDS infrastructure (i.e. will specified software agents need to be installed)	
Conform that you can meet the services level agreements which are proposed in the tender as well agreeing to the fees at risk If your proposed service level agreements or fees at risk differ please outline what you are proposing in relation to • Hours of Services • Incident Severity Levels • Response times • Resolution Times • Escalation Process • Fees at risk	
indicate if staff who will be providing the service will be ITIL certified.	

Information Requested	Response
Please provide details of how you propose to deliver service improvements and how service improvement is to be measured.	
Outline any services which are explicitly excluded from your offering	

Backup

Information Requested	Response
Provide an overview of the solution which is proposed for backup as a service	
Provide details of the datacentre infrastructure which will be used to support the backup solution. Provide details of the Tier level (Uptime Institute) of the data centre	
Outline any capacity limits which if exceeded would require the pricing to flex	
Provide a description of the encryption and security mechanisms for data while in transit and at rest	
Provide a description of how the backup operation will be managed and monitored including how back integrity will be ensured	
Outline any services which are explicitly excluded from your offering	

Disaster Recovery

Information Requested	Response
Provide an overview of the solution which is proposed for disaster recovery as a service clearly outlining how the required RTO and RPO's will be met	
Provide details of the datacentre infrastructure which will be used for the	

Information Requested	Response
disaster recovery solution. Provide details of the Tier level (Uptime Institute) of the data centre	
Outline any capacity limits which if exceeded would require the pricing to flex (for example of the DR was invoked and used for a period of time)	
Provide a description of the encryption and security mechanisms for data which will be replicated to the cloud to support the DR solution	
Provide a description of how the DR solution will be managed and monitored	
Please indicate what DR testing support will be provided and at what frequency	
Provide details of how the DR service can be invoked	
Outline any services which are explicitly excluded from your offering	

Security Assessment

Information Requested	Response
Outline your overall approach to the security assessment	
Detail the specific vulnerability and penetration tests which will be carried out	
Provide details on the tools which will be used to carry out the testing. Please note that the RDS require that any data collected as part of this exercise must be securely stored and deleted when the exercise is completed	
Provide a table of contents for the assessment report	

Professional Services

Information Requested	Response
Outline the proactive measures which will be taken to support RDS in the development of their future ICT roadmap	
Provide man days rates Hourly Rates will be calculated by dividing the Day Rate by 8) for the various grades. This should include: a) Network Engineer b) Security Specialist c) Database Systems Administrator d) Helpdesk Support e) Wintel Server Engineer / Administrator f) Wintel System Specialist / Engineer g) Citrix System Specialist / Engineer h) VMWare System Specialist / Engineer i) Business Analyst j) Project Manager	See Excel Cost Template for response
Provide sample CV's for key roles	
Outline what value-added services you can provide to the RDS	

Additional Services

Information Requested	Response
Outline any infrastructure projects which are proposed to improve the infrastructure	

Transition Plan

Information Requested	Response
Provide a transition plan to move from the existing service provider who currently provides similar scope managed services to the RDS. The plan should clearly identify • The roles and responsibilities of RDS and the Service provider • The Service provider team which will be involved in the transition • An indicative timeline for the transition • The RDS resources which will be required • The current service provider resources which will be required • A list of key documents which will be required from the current service provider	
Identify any potential risks and migration actions in the transition	
Provide details of what exit services you will provide at the end of the contract in order to transition to another provider. Please refer to schedule 4 for the RDS expectations	

References

Please supply a list of clients similar in size to the RDS where you are providing similar services.

Please complete the following table for a minimum of three reference sites There is a preference for reference sites which are

- Similar in nature to RDS
- Have a virtualized server and desktop environment
- Have cloud based back up and disaster recovery included in the scope
- Using 24X 7 support

Information Required	Responses
Customer Name and Address	
Contact Details (name, e-mail, phone no)	
Type and Description of Customer	
Overall scope of the Managed Service	
Defined Service Levels	
Date the Contract started	

Cost

The Pricing matrix provided in Schedule 3 in Excel must be completed and returned. An excel version of the matrix will be provided upon notification to the RDS of intention to submit a tender.

Evaluation Criteria

The tenders will be evaluated according to the criteria in the table below.

Criteria	Marks Available
Quality of the proposed Service and Service Level Agreement • Managed ICT Service • Backup as a Service • Disaster Recovery as a Service • Security Services • Professional Services	500
Transition Plan	50
References	100
Agreement on the RDS Services Framework	50
Cost	300

Non-Cost Award Criteria

Non-cost award criteria will be awarded marks using the following methodology:

A 5-mark system will be used. A mark will be awarded to each criterion from 0 to 5. This mark, or multiplier, will be used to calculate the score to be awarded.

Non-Cost Award Criteria	Multiplier
Excellent: Excellent response with very few or no weaknesses that exceeds requirements, and provides comprehensive, detailed, and convincing assurance that the Tenderer will deliver to an excellent standard.	5
Very Good: A very good response that demonstrates real understanding of the requirements and assurance that the Tenderer will deliver to a high standard.	4
Good: A satisfactory response which demonstrates a reasonable understanding of requirements and gives reasonable assurance of delivery to an adequate standard but does not provide sufficiently convincing assurance to award a higher mark.	3
Poor: A response where reservations exist. Lacks full credibility/convincing detail, and there is a significant risk that the response will not be successful.	2
Very Poor: Response fails to address the criterion under consideration	1

Example:

For example, if a score of 300 is available, the base score is 60 (300/5). If the Tenderer is marked 5 (excellent), a score of 300 marks will be awarded (60 x 5). If the Tenderer is marked 2 (fair), a score of 120 marks will be awarded (60 x 2).

Cost Award Criteria

Cost Award Criteria will be awarded marks using the following methodology

The Tenderer whose Cost is the lowest shall be awarded the maximum marks available for Pricing, all other Tenders shall be marked relative to the lowest Ultimate Cost using the following formula:

$$\frac{\text{(The lowest Cost tendered) * (Maximum mark available for Pricing)}}{\text{Cost of Tender being evaluated for Pricing}}$$

Schedules

Schedule 1 - Specification RACI Table
Schedule 2 - Services Level Agreements and Service Credits
Schedule 3 - Pricing
Schedule 4 - Transfer and Exit Services

Schedule 1 Specification RACI Tables

The following RACI tables identify activities and respective roles and responsibilities of each Party in performing and delivering the Services as defined in this Schedule. The scope of each activity is in relation to the Service Environment as defined in this Schedule.

General

Table 1 – General Roles and Responsibilities

General Roles and Responsibilities			Recipient	Provider
Pre-Implementation				
		Plan and coordinate the resources and capabilities needed to enable the smooth operation of the service transition stage	CI	AR
		Plan and coordinate individual service transitions,	CI	AR
		Undertake configuration management planning	I	AR
		Release and deployment policy and planning	A	R
Operations				
		Manage service provision	A	R
		Manage outsource contracts	AR	CI
		Provide technical guidance and specialist support	CI	AR
		Monitor and measure performance and availability	CI	AR
		Measure process and service CSFs and KPIs	CI	AR
		Report on performance and availability	CI	AR
		Report on CSFs and KPIs	CI	AR
		Report on service management failures and performance	CI	AR
		Report on root cause analysis and improvements	CI	AR
End of Table				

Capacity Management

Capacity management includes business, service and component capacity management across the service lifecycle.

Table 2 – Capacity Management Roles and Responsibilities

Capacity Management Roles and Responsibilities			Recipient	Provider
		Prepare and maintain capacity plan	A	R
		Define forward requirements for capacity with sufficient time to incorporate procurement	CI	AR
		Procure hardware and systems software as necessary to meet capacity plan	AR	CI
		Monitor and optimise resource utilization	I	AR
End of Table				

Availability Management

The purpose of availability management is to provide a point of focus and management for all availability-related issues that apply to services, components and resources, ensuring that availability targets in all areas are measured and achieved, and that they match or exceed the current and future agreed needs of the business in a cost-effective manner.

Table 3 – Availability Management Roles and Responsibilities

Availability Management Roles and Responsibilities			Recipient	Provider
		Formulate availability and recovery design criteria	A	R
		Maintain availability plan	A	R
		Define targets for availability	AR	CI
		Monitor availability and report on trends	CI	AR
		Analyse events, incidents and problems involving service unavailability to identify root causes and improvement opportunities	I	AR
End of Table				

Service Asset and Configuration Management

The purpose of service asset and configuration management (SACM) is to ensure that the assets required to deliver services are properly controlled, and that accurate and reliable information about those assets is available when and where it is needed. This information includes details of how the assets have been configured and the relationships between assets.

Table 4 – Service Asset and Configuration Management Roles and Responsibilities

Service Asset and Configuration Management Roles and Responsibilities			Recipient	Provider
		Identify configuration items	I	AR
		Establish and maintain CMDB	I	AR
		Control configuration	I	AR
		Maintain and track CI status	I	AR
		Verify and audit CIs against CMDB records	I	AR
End of Table				

Release and Deployment Management

The purpose of the release and deployment management process is to plan, schedule and control the building, testing and deployment of releases for infrastructure components. The scope does not include major upgrades which will be managed as projects.

Table 5 – Release and Deployment Management Roles and Responsibilities

Release and Deployment Management Roles and Responsibilities			Recipient	Provider
		Release and deployment design, build, configuration and documentation	CI	AR
		Release testing and acceptance	CI	AR
		Release sign-off	AR	I
		Release review	CI	AR
End of Table				

Event Management

Effective service operation depends upon knowing the status of the infrastructure and the components within.

Table 7 – Event Management Roles and Responsibilities

Event Management Roles and Responsibilities			Recipient	Provider
		Detect events from monitoring tools	I	AR
		Classify event as informational, warning or exception	I	AR
		Determine appropriate response and control action based on event type and related CI and service impact	I	AR
		Take action or escalate to incident, problem or change management	CI	AR
End of Table				

Incident Management

The purpose of incident management is to restore normal service as quickly as possible and to minimize the adverse impact on business operations. 'Normal' service is the level of service agreed and defined within the SLAs and OLAs.

Table 8 – Incident Management Roles and Responsibilities

Incident Management Roles and Responsibilities			Recipient	Provider
		Record incidents	I	AR
		Incident investigation and diagnosis	I	AR
		Assign ownership	I	AR
		Incident resolution and recovery	I	AR
		Root Cause Analysis	I	AR
		Incident closure	I	AR
End of Table				

Problem Management

The purpose of problem management is to manage the lifecycle of all problems, from first identification through investigation and documentation to eventual removal.

Table 9 – Problem Management Roles and Responsibilities

Problem Management Roles and Responsibilities			Recipient	Provider
		Identify and record problems	I	AR
		Classify and prioritise problems	A	R
		Root Cause Analysis	IC	AR
		Record problem resolution and close out	I	AR
		Analyse trends, support requirements and preventative actions	I	AR
		Provide management information	CI	AR
		Categorise and document errors, problems and workarounds in knowledge base	I	AR
		Undertake major problem reviews	CI	AR
End of Table				

Service Desk Function

Table 10 – Service Desk Function Roles and Responsibilities

Service Desk Function Roles and Responsibilities			Recipient	Provider
		Resource and manage service desk effectively	I	AR
		Define responsibilities and resolution pathways	CI	AR
		Monitor workload		AR
		Produce management reports	CI	AR
End of Table				

IT Operations Management Function

Table 11 – IT Operations Management Function Roles and Responsibilities

IT Operations Management Function Roles and Responsibilities			Recipient	Provider
		Manage ICT infrastructure events	I	AR
		Workload management and scheduling		AR
		Manage storage, backup and recovery operations	CI	AR
		Maintain operation documentation and procedures		AR
End of Table				

Schedule 2 Service Level Agreements and Service Credits

Introduction

This Schedule sets out the Service Level Requirements (SLRs) that will apply to the Services provided and delivered under the Agreement as specified, together with the means by which Fee Reductions are calculated for failure to comply with the SLRs.

Calculation of Fee Reductions

The Fee Reductions in respect of any non-performance of the Services to the standard specified by these SLRs shall be calculated as follows:

- The Fees at Risk will be 20% of the monthly Fees. In this regard "Fees at Risk" means the total amount of the Fees which may be deducted in any single month for failure to comply with the SLRs listed at Section 4 below.
- The proportion of the Fees at Risk allocated to each of the SLR categories listed in the tables in Section 4 below are as follows:

SLR category	**SLA % Allocation**
Incident Handling SLRs	
Failure to Meet Severity 1 Response Levels	20%
Failure to Meet Severity 1 Resolution Levels	40%
Failure to Meet Severity 2 Response Levels	5%
Failure to Meet Severity 2 Resolution Levels	25%
Failure to meet DR RTO and RPO's	10%
Total	
TOTAL ALLOCATION	**100%**

Termination

On the third consecutive Failure for any individual SLR, the Agreement shall be considered in default, and Recipient will be entitled to terminate the Agreement.

"Failure" in this regard means in respect of an SLR identified in Section 4 below, the failure to meet the relevant SLR Target in accordance with the SLR Reporting Internal, provided that no Provider Relief event applies.

Service Level Requirements

The following tables define the SLRs that will apply to the Services:

Incident Handling Service Levels

Incident Handling SLRs	
Incident Response – Severity 1 and 2	
SLR Measure	
SLA % Measure = (Number of Incidents in the SLA Measurement Interval that were responded to in the time allocated in SLA Minutes Measure between incident notification to Supplier and Supplier notification of Recipient) / (Number of Incidents in the SLA Measurement Interval) * 100	
Provider Relief	
Recipient does not follow agreed incident logging procedures for phone, email, system logging.	
SLR Measurement Interval	SLR Reporting Interval
Daily	Weekly
SLR Target	
Severity 1 <=15 minutes average response 95% 30 minutes max response 100% Severity 2 <=120 minutes average response 95% 150 minutes max response 100%	
Incident Resolution Severity 1	
SLR Measure	
SLA % Measure = (Number of Severity 1 incidents during agreed hours in the SLA Measurement Interval that were closed within the SLA Hours Measure) / (Number of Severity 1 incidents during agreed hours in the SLA Measurement Interval) *100	
Provider Relief	
Time waiting on Recipient or third-party response	
SLR Measurement Interval	SLR Reporting Interval
Daily	Weekly
SLR Target	
95% within 2 hours 100% within 8 hours	
Incident Resolution Severity 2	
SLR Measure	
SLA % Measure = (Number of Severity 2 incidents during agreed hours in the SLA Measurement Interval that were closed within the SLA Hours Measure) / (Number of Severity 2 incidents during agreed hours in the SLA Measurement Interval) *100	
Provider Relief	
Time waiting on Recipient or third-party response	
SLR Measurement Interval	SLR Reporting Interval
Daily	Weekly

	SLR Target	
		95% within 8 hours 100% within 24 hours
End of Table		

[1] “Severity 1” means the system, service, Work Product, function or business process is rendered inoperable and/or tests cannot be continued or performed in an adequate manner in which event a work around (or back-out) shall be provided immediately by Provider

[1] “Severity 2” means the system, service, Work Product, function or business process is unusable preventing it from reaching the right result as expected with the system, service or Work Product for the impacted function(s); this/these functions is/are not operational but the other functions can still be used, or the use is otherwise significantly impacted (for example a significant group of end users impacted with serious degradation of the Services)

Schedule 3 Pricing

See attached Excel Spreadsheet

Schedule 4 Transfer and Exit Services

This schedule provides a description of the transfers and exit service requirements in the event that the provisions of the services transitions to the RDS or another Service Provider. The schedule provides for circumstances where Recipient or Provider is terminating the Agreement. It summarises the transfer of services and assets, financial considerations and the roles and responsibilities of both parties.

The schedule also addresses 'Disentanglement', which is complete transition of the services being terminated from Provider and the Subcontractors to Recipient, or to any persons nominated by Recipient to replace Provider, without any interruption of or adverse impact on the services or any other services provided by third parties. This may be due to the expiration of the contract or any other reason anticipated in the Agreement

Service Definitions

Table 2 – Definitions

Definition of Terms Used Within Exit Planning Framework	
Effective Date (ED)	The effective start date of the Services within scope of the Transfer or Exit
Exit Notice Date (END)	The date exit is notified
Termination Notice Period	Means the length of time either party must provide to the other party to notify the intent to terminate.
Disentanglement Period or Exit Assistance Period	Means the period immediately following expiry of Termination Notice Period.
Exit Plan	The overall plan for completing the transfer of the services to Recipient (or a Replacement Provider).
Exit Transition Plan	The plan for transitioning Services from Provider to Recipient (or a Replacement Provider).
Exit Assistance	Means the assistance and other activities as each is to be provided by Provider to support the orderly handover to the new Provider or to Recipient (take services 'in-house'). At a minimum it will include: • Responsibilities described in Section 2 – Transfer and Exit Services of this Schedule; • Full co-operation during any 3rd party Provider selection process, including information provision for SOW, SLAs, etc. required for RFP, contract drafting and due diligence by Recipient and 3rd party Providers (support for minimum 2 provider due diligence processes); • Transition planning with Recipient and 3rd party Provider; • Transition over a period of 2 months following handover of services to either Recipient or 3rd party Provider.
Exit Deliverables	Deliverables produced to facilitate exit or transfer, as summarised in Attachment 6.1
Exit Transition Plan Date (ETP)	The commencement date of the Exit Transition Plan for transitioning to Recipient or a Replacement Provider
Services Expiry Date (SED)	The date upon which the Services within scope of the Transfer or Exit will expire, expected to be upon the conclusion of the Exit Plan

General Responsibilities

- Provider shall provide support to Recipient during a transition, transfer or exit to ensure that the service levels to Recipient are not unduly affected
- The following general guidelines will be followed:
    - Each party will, in consultation with the other party, take all commercially reasonable steps to minimise negative business and/or financial impact on the other party arising from the transfer of the Services;
    - Provider and Recipient will provide to each other and to any new Provider, all information needed for Disentanglement, including data conversion, interface specifications, and related professional services, subject to the confidentiality provisions and security provisions in the main body of this Agreement and provided that Provider is under no obligation to disclose any of its or its subcontractor's trade secrets.
    - Provider will discharge its duties under this Agreement in such a way as to ensure that Disentanglement can be carried out without encountering hindrances, including those highlighted in the preceding 2 paragraphs.

General Principles

The following sections outline the principles upon which termination will work. The detail is contained in Section 2 – Transfer and Exit Services.

General Termination Requirements

- Provider will continue to provide the contracted operational services during the Exit Assistance Period until successfully transferred and receive payment for such services according to the terms of the Agreement and associated schedules.
- Provider will arrange the assignment and/or transfer to Recipient or its replacement Provider of all such third-party contracts as are used exclusively in the provision of the services to Recipient client accounts.

Termination for Force Majeure Event

- Provider will provide Exit Assistance to Recipient. Exit assistance period will be agreed in the Exit Plan, and will be no longer than 2 months, and at a minimum cover the activities set out in the definition of Exit Assistance.
- All other clauses under 'General Termination Requirements' apply, where such clauses do not conflict with clauses under this heading.

Termination for Breach or Cause where Provider is the Defaulting Party

- Provider will provide Exit Assistance to Recipient. Exit assistance period will be agreed in the Exit Plan, and will be no longer than 3 months, and at a minimum cover the activities set out in the definition of Exit Assistance.
- All other clauses under 'General Termination Requirements' apply, where such clauses do not conflict with clauses under this heading.

Termination for Breach or Cause where Recipient is the Defaulting Party

- Provider will provide Exit Assistance to Recipient. Exit assistance period will be agreed in the Exit Plan, and will be no longer than 3 months, and at a minimum cover the activities set out in the definition of Exit Assistance.

- All other clauses under 'General Termination Requirements' apply, where such clauses do not conflict with clauses under this heading.
- All Intellectual Property Rights in or to the Work Products, where the Intellectual Property Rights are still with the Provider, stay with the Provider until all undisputed payments are received according to the Agreement,

Termination for Convenience by Recipient

- Transfer services commence only at the end of the termination period, they are commonly agreed together with the related payments in case of a termination and not related to or covered by this agreement.
- Provider will provide Exit Assistance to Recipient, assuming no undisputed payments are delayed.
- Exit Assistance Period will be agreed in the Exit Plan, and will be no longer than 3 months, and at a minimum cover the activities set out in the definition of Exit Assistance.
- All other clauses under 'General Termination Requirements' apply, where such clauses do not conflict with clauses under this heading.

TRANSFER AND EXIT SERVICES

Roles and Responsibilities

The scope of activities in this Schedule is based on defined roles and responsibilities of each Party as defined in this Section, using tables of activities and RACI roles and responsibilities. The RACI roles and responsibilities shall be interpreted as follows:

- **R**esponsible: Party is Responsible and must perform action
- **A**ccountable: Party is Accountable and must make decisions
- **C**onsulted: Party is Consulted and is expected to perform any actions required to input to this activity and decisions
- **I**nformed: Party is Informed of activity and decisions, and must incorporate such information into its own activities and planning

Table 3 – Transfer and Exit Roles and Responsibilities

Transfer and Exit Roles and Responsibilities			Recipient	Provider
At Effective Date				
		Produce Exit Deliverables as defined in this annex within 3 months	CI	AR
		Review and approve Exit Deliverables every 6 months	A	R
		Comply with principles in this Schedule	AR	AR
At Exit Notice Date				
		Develop transition service request	AR	CI
		Prepare Exit Plan and proposal, including: • Assist in the preparation of that portion of the transition plan detailing Provider responsibilities, including schedules and resource commitments.		AR

		• Provide to Recipient documentation used by Provider to provide the services, including up to date operating procedures, backup and technical documentation. • Perform a formal handover of the operations procedure manual, used to perform the services, to Recipient's operations staff or designees. • Identify, record and provide release levels for system software and associated software libraries. • Provide assistance to Recipient in notifying third party suppliers of the procedures to be followed during the transition. • Identify and explain naming conventions. • Assist Recipient in its analysis of the space required for software and data file libraries. • Co-operate with Recipient in the preparation and conduct of transition testing. • Provide asset listings for all equipment and other assets used by Provider primarily to perform the services for Recipient. • Provide copies of all Provider and third-party software manuals and other documentation within the possession or control of Provider that are required by Provider and that are relevant to the services, to the extent permitted by those third-party software vendors.		
		Evaluate Exit Plan and proposal	AR	
		Approve Exit Plan	AR	
During Exit Assistance Period				
		Execution of transition services as per Exit Plan	AR	AR
		Produce Exit Deliverables as defined in this annex		AR
		Minimise disruption to Services		AR
		Cooperate with Recipient (or Replacement Provider as appropriate) to avoid any Service disruption		AR
		To the extent requested by Recipient, assign, novate or transfer, or procure the sale, assignment, novation or transfer, of the Service Assets to Recipient and/or Replacement Provider		AR
		Return all Recipient data and other Recipient confidential information.		AR
		Remove all requested Recipient data files and other Recipient confidential information from its possession.		AR
		Deliver to Recipient Recipient’s data files and other Recipient confidential information stored on desktop computers and servers for which Provider is responsible, including backup tapes.		AR
		Deliver to Recipient, on media and in formats specified by Recipient, all Recipient Data in Provider's or its Subcontractors' possession or control.		AR
		Provide all information regarding the services or as otherwise needed for transfer,		AR
	Transfer of Assets			
		Provide all Recipient data and software owned by or proprietary to Recipient or in respect of which it has any right to use pursuant to the provisions of this agreement or in law.		AR
		Provide service assets and other such assets as Recipient selects to transfer to Recipient or its designee, including from among those assets located at any Recipient Facility or Premises and held by Provider and for the provision of services largely to Recipient, at a price that is the lesser of the net book value or the fair market value of those assets selected.		AR
		Promptly remove from the Premises any of Provider’s assets that Recipient, or its designee, chooses not to purchase excluding Provider assets used to supply service to 3rd Party Clients.		AR

	Transfer of Contracts		
	Use all reasonable endeavours to procure at no charge to Recipient any third party authorisations necessary to grant Recipient the use and benefit of any third-party contracts between Provider and third-party contractors used to provide the services, pending their assignment to Recipient. Recipient will be responsible for procuring licences to any tools used by Provider to provide service.		AR
	Transfer of Skills		
	Use all reasonable efforts to transfer the skills necessary to Recipient to continue support of the systems.		AR
	Take responsibility for subcontractor obligations upon termination		AR
	Access to Systems		
	Provide Recipient reasonable access to, and use of, equipment, software, personnel, third parties, and other resources used by Provider to provide the services (collectively 'systems'), and provide to Recipient reasonable information concerning such systems, all as necessary for the transition		AR
End of Table			

EXIT DELIVERABLES

The following table contains the list of Deliverables that must be maintained to support the Transfer and Exit activities and responsibilities defined in this Schedule.

Table 3 – Exit Deliverables

Deliverable	Key Activity	Purpose
1 Exit Strategy	Plan for handover of responsibility for the Services.	transition
2 Infrastructure Design	A repository of the infrastructure design and composition of the Infrastructure.	transition so that suitably skilled personnel will be able to operate and support the technical infrastructure
3 Configuration Management	A register of all the tangible assets of the environment: 4.1 hardware asset register 4.2 software licences 4.3 applications register	knowledge transfer and transition, definition of assets to be transferred
4 Third Party Agreements	A detailed list of all third-party agreements relating to the provision of the Services.	knowledge transfer and novation preparation and action (where appropriate)
5 Contract Novation	To assess the capability for novation of third-party contracts and to produce a plan of activities for Novation	knowledge transfer and completion of novation process where permitted by third party
6 Key Contacts List	Contact names and details for the key partners, sub-contractors and Provider staff	transition communications aid
7 Work in Progress	Details of any project services and/or other T&M based services or support, in progress on the start of the Exit Transition Plan - implementation of this project	knowledge transfer and transition

Deliverable	Key Activity	Purpose
8 Resource Usage	Resource levels employed by Provider in the previous 12 months	knowledge transfer, transition and TUPE
9 Return of Data & Property	A list of any property, documentation, data or other items belonging to one party but in the possession of the other, and agreed plans for return or destruction as appropriate	knowledge transfer, transition and exit strategy
End of Table		

Annexures

Annex 1 – Infrastructure Inventory
Annex 2 – Backup Schedule

Annex 1 – Infrastructure Inventory

See attached Excel spreadsheet

Annex 2 – Backup Schedule

See attached Excel spreadsheet