UNIVERSITY OF THE
WITWATERSRAND,
JOHANNESBURG

Annexure 1: Scope of work for the Information Service Management Tool (Help desk Tool)

The purpose of the University acquiring the solution/system is to satisfy the following objectives:
Have a single point of entry for service requests (which includes the logging of incidents and change requests) and have the ability to route the requests to the relevant faculty, division or department and within each unit.
Effectively manage service requests
Create and manage a knowledge base for efficient management of services.
Dashboards for monitoring and management
To have reporting capabilities
To have survey capabilities
BI and Library requested capability for separate configuration and customisation for their particular areas

The solution/system will be supplied and the services delivered substantially in accordance with the timelines set out in this scope of work.

University's Objectives

The scope of the RFI entails the ICT's requirements around the acquisition and deployment of an IT Service Management Tool (Software) to support ICT's adoption of the following IT Service Management) processes:

- Incident Management
- Service Request Management
- Service Level Management
- Service Catalogue Management
- Problem Management
- Change Management
- Release and Deployment Management
- Configuration Management
- Auto Attendant for Service Desk

The supplier must, in view of the previously mentioned, be adequately experienced and competent in the IT Service Management (ITIL) tool to provide for the specific needs required.

1. Project Description

The aim of the project is to source; implement one ITSM tool that will be used across the University as a single point of entry for logging service requests and to device an optimal and efficient method of routing tickets to the correct faculty, division and department for resolving. To have the ability to monitor tickets for better and more efficient service delivery to customers/clients, and perform statistical reporting. The tool should have survey capabilities. An Auto attendant option should be included.

2. Solution/System Specifications

The description and specifications of the solution/system are:

- **ITSM Incident Management Incident management procedure**
    - The activities within the incident management process include:
    - Incident detection and recording
    - Incident reporting and communication
    - Priority Classification and initial support
    - Investigation and analysis
    - Resolution and record
    - Incident closure
    - Incident ownership, monitoring, tracking and communication
    - Establish incident framework management
    - Evaluation of incident framework management
- **ITSM Problem Management**
        - Targeting support action
        - Providing information to the organization
        - Problem identification and recording
        - Problem classification
        - Problem investigation and diagnosis

- **ITSM Request Fulfilment (To ensure formalised request classification, logging, recording, authorisation, fulfilment, and reporting)**

Request for Service

A formal request from a user for something to be provided – for example, a request for information or advice; to reset a password; or to install a workstation for a new user. The details of a Request for Service are recorded by Request Fulfilment in a Service Request Record.

Service Request Model

A (Service) Request Model defines specific agreed steps that will be followed for a Service Request of a particular type (or category).

Service Request Record

A record containing all details of a Service Request. Service Requests are formal requests from a user for something to be provided – for example, a request for information or advice; to reset a password; or to install a workstation for a new user.

Service Request Status Information

A message containing the present status of a Service Request sent to a user who earlier reported requested a service. Status information is typically provided to users at various points during a Service Request's lifecycle.

- **ITSM Change Management (To ensure requesting, recording, assessing, approval, implementation & review of changes in a formal, structured, controlled and accountable manner)**

Change Management Support

Process Objective: To provide templates and guidance for the authorization of Changes, and to supply the other IT Service Management processes with information on planned and ongoing Changes.

Assessment of Change Proposals

Process Objective: To asses Change Proposals which are typically submitted for significant Changes by Service Strategy. The purpose of assessing Change Proposals is to identify possible issues prior to the start of design activities.

RFC Logging and Review

Process Objective: To filter out Requests for Change which do not contain all information required for assessment or which are deemed impractical.

Assessment and Implementation of Emergency Changes

Process Objective: To assess, authorize and implement an Emergency Change as quickly as possible. This process is invoked if normal Change Management procedures cannot be applied because an emergency requires immediate action.

Change Assessment by the Change Manager

Process Objective: To determine the required level of authorization for the assessment of a proposed Change. Significant Changes are passed on to the CAB for assessment, while minor Changes are immediately assessed and authorized by the Change Manager.

Change Assessment by the CAB

Process Objective: To assess a proposed Change and authorize the Change planning phase. If required, higher levels of authority (e.g. IT Management) are involved in the authorization process.

Change Scheduling and Build Authorization

Process Objective: To authorize detailed Change and Release planning, and to assess the resulting Project Plan prior to authorizing the Change Build phase.

Change Deployment Authorization

Process Objective: To assess if all required Change components have been built and properly tested, and to authorize the Change Deployment phase.

Minor Change Deployment

Process Objective: To implement low-risk, well-understood Changes which do not require the involvement of Release Management.

Post Implementation Review and Change Closure

Process Objective: To assess the course of the Change implementation and the achieved results, in order to verify that a complete history if activities is present for future reference, and to make sure that any mistakes are analysed and lessons learned.

- **ITSM Release and Deployment Management (To ensure requirements management, requesting, recording, building, testing, and deployment of releases in a formal, structured, controlled, and accountable manner)**

Release Management Support

Process Objective: To provide guidelines and support for the deployment of Releases.

Release Planning

Process Objective: To assign authorized Changes to Release Packages and to define the scope and content of Releases. Based on this information, the Release Planning process develops a schedule for building, testing and deploying the Release.

Release Build

Process Objective: To issue all necessary Work Orders and Purchase Requests so that Release components are either bought from outside vendors or developed/ customized in-house. At the end of this process, all required Release components are ready to enter the testing phase.

Release Deployment

Process Objective: To deploy the Release components into the live production environment. This process is also responsible for training end-users and operating staff and circulating information/ documentation on the newly deployed Release or the services it supports.

Early Life Support

Process Objective: To resolve operational issues quickly during an initial period after Release deployment, and to remove any remaining errors or deficiencies.

Release Closure

Process Objective: To formally close a Release after verifying if activity logs and CMS contents are up to date.

- **ITSM Problem Management (To ensure problem recording, prioritization, classification, updating, escalation, resolution and closure in a formal, structure, controlled and accountable manner. To provide, maintain and populate an information system [known error database] for purposes of addressing problems areas either before of after occurrences).**

Proactive Problem Identification

Process Objective: To improve overall availability of services by proactively identifying Problems. Proactive Problem Management aims to identify and solve Problems and/or provide suitable Workarounds before (further) Incidents recur.

Problem Categorization and Prioritization

Process Objective: To record and prioritize the Problem with appropriate diligence, in order to facilitate a swift and effective resolution.

Problem Diagnosis and Resolution

Process Objective: To identify the underlying root cause of a Problem and initiate the most appropriate and economical Problem solution. If possible, a temporary Workaround is supplied.

Problem and Error Control

Process Objective: To constantly monitor outstanding Problems with regards to their processing status, so that where necessary corrective measures may be introduced.

Problem Closure and Evaluation

Process Objective: To ensure that - after a successful Problem solution - the Problem Record contains a full historical description, and that related Known Error Records are updated.

Major Problem Review

Process Objective: To review the resolution of a Problem in order to prevent recurrence and learn any lessons for the future. Furthermore it is to be verified whether the Problems marked as closed have actually been eliminated.

Problem Management Reporting

Process Objective: ITIL Problem Management Reporting aims to ensure that the other Service Management processes as well as IT Management are informed of outstanding Problems, their processing-status and existing Workarounds.

• **ITSM Service Catalogue Management, enabled by clarification of ICT Service Bundles (To provide a structure document that contains information about all services on offer by ICT. Will clarify service descriptions, customer responsibilities, any applicable metrics, and will assist with classification / categorisation of Incidents, Service Requests and Change Requests).**

- ordering and requesting processes
- prices
- deliverables
- contact points

• **ITSM Configuration management (To support and ensure asset and configuration planning, identification, classification, as well as management and control over asset and configuration information in the appropriate data repositories [Configuration Management Data Base]).**

Configuration management is the management and traceability of every aspect of a configuration from beginning to end and it includes the following key process areas under its umbrella:

- Identification
- Planning
- Change control
- Change management
- Release management
- Maintenance

ITSM Events management

The purpose is the ability to detect events, investigate and determine the correct control action

The events (warnings and exceptions) can be used to automate many routine activities

Event Management can be applied to any aspects of Service Management that can be controlled and can be automated (Configuration Items)

Provide mechanisms for early detection of incidents.

Some types of automated activities can be monitored by exception, reducing downtime.

Achievement of the aforesaid objectives is, in many instances, dependant on business systems, information systems, and technology architectures that will culminate in automation of many activities supporting the above-mentioned processes.

Not only is aforesaid process automation a ICT requirement, but more so the requirement to –

- Acquire an ITSM Tool that has grown beyond basic service desk and "trouble ticketing" features to an ITSM tool that supports and enables a much broader array of ITSM.
- Acquire an ITSM Tool that provides for out-of-the-box features and functionality, ease of administration, support, configuration and customization, as well as scalability.
- Acquire the services of an ITSM vendor that supports a partnership founded on an enhanced customer experience, agreed upon service levels and performance metrics.
- Acquire the services of an ITSM vendor which is well-positioned with its product portfolio, and therefore likely to continue to deliver ITSM tools, ITSM tool functionality, and associated services.
- That is well priced, and supports ICT's plan to achieve cost effective (new) implementation and execution rather than attempting to upgrade the existing ITSM tool that provides limited functionality.

- **Auto Attendant**
    - When you call the service desk, there should be automatic routing options to direct your call

Support and Maintenance and associated service levels are:

Internal Application Support Team

a. The teams' application management and maintenance activities will be consistent with the application management function.
b. AST (service desk) will function as the service desk for the application within their scope of responsibility.
c. AST (service desk) will act as the single point of contact for the work events associated with the application.
d. AST (technical team) will be responsible for managing application enhancements and maintenance requests through their entire lifecycle.
e. AST (technical team) has to ensure that the application is available to the users during the required hours of operation.

External Application Support Team

a. The service provider should be able to offer support in the following areas:
    - Service functionality – should the AST (technical team) not be able to resolve the issue(s) internally, support should be given
    - Service availability and reliability – any technical and complex issues that might arise whereby the internal ATS cannot restore the availability of the application within the defined OLA's, the SLA's pertaining to this should be triggered
b. A clear and defined SLA will be created and agreed on between the Service Provider and the University

3. Standards

ISO 9001
COBIT
ICASA
ISACA
ITIL

4. Training

The Supplier will provide the following training (training needs will be better defined at the start of the Project):

a. End-users of the system (i.e. the call centre agents that will be logging the calls)
b. Electronic HOW-TO guide for users
c. Administrative and technical training for the back-end support (for the internal application support team.

5. Service Provider Responsibilities

The Service Provider will:

a. Designate its Project Manager for this Agreement (Service Provider Representative). The Service Provider may from time to time and on written notice designate other persons to act as its Representative. This Representative will liaise with the University as often as required for the efficient implementation of the Project and is authorised to transmit instructions from the Service Provider to the University. To receive information from the University, submit to the University reports as appropriate, which may include partial reports released from time to time at dates as may be designated in the Scope of Work,
b. Assign a personnel complement sufficient both in numbers and skills to ensure due and proper performance of its obligations under this Agreement,

c. Perform the Services with due care and skill and in accordance with the degree of skill, care and diligence normally exercised by recognised professional persons or firms who supply Services of a similar nature,
d. If and whenever the University gives it written notice of any deficiencies in performing its obligations hereunder, acknowledge such notice in writing within 5 days,
e. Provide continued training and development for all of its personnel in those skill areas relevant to the performance by the Service Provider of its obligations under this Agreement,
f. Ensure that the Goods and Services will be fit for the purposes for which these types of Goods and Services are commonly required and for any other purposes described in this Agreement,
g. Ensure that it and its personnel comply with all applicable laws and the University's rules, regulations and policies, procedures and standing orders, as may be amended from time to time. Without limiting the generality of this, the Service Provider must comply with applicable legislation relating to the rendering of the Services and delivery of the Goods,
h. Be solely responsible for, and carry all risk for, a designated lockable storage container, such as a secure cupboard, as well as its contents (which includes replaceable parts and the like), that is placed on the University's premises and managed by the Service Provider, and
i. Keep statistics, minutes and other records required by legislation on file and available for inspection by the University is appointed administrator or auditor.
j. Should be ISO 9001 compliant
k. Should provide a letter from the OEM
l. Should provide evidence of proven track record and experience
m. Should provide ICASA certification that the tool needs
n. Should provide skills transfer
o. System integration to Active Directory (AD)

6. University Responsibilities

The University will:

a. Designate its Supply Manager and its Project Manager (**University Representative**) for this Agreement. The University may from time to time and on written notice designate another person to act as its Representative. This Representative will liaise with the Service Provider as often as required for the efficient implementation of the Project and is authorised to transmit instructions from the University to the Service Provider, and to receive information from the Service Provider,
b. Either directly, or through the University Representative, instruct the Service Provider regarding the University's requirements in connection with the Project. The University Representative is authorised to define and interpret the University's requirements regarding the Goods and Services and convey decisions pursuant to the Project to the Service Provider and to receive information from the Service Provider on behalf of the University,

c. Provide the Service Provider with such access as may be necessary to deliver the Goods and to enable the Service Provider to perform the Services required of the Service Provider for the purposes of the Project,
d. Make available all information as may be necessary to enable the Service Provider to fulfil its obligations under this Agreement,
e. Give written notice to the Service Provider if and whenever it becomes aware of any deficiencies in the Services provided hereunder, and
f. Pay the Service Provider as provided for in this Agreement.

7. Deliverables and Delivery Schedule

The Deliverables and associated delivery dates under this Agreement are:

a. Deliverable 1 – Phase 1 (Wits ICT - Service Delivery) (by Milestone Date 7/12/2018):

b. Deliverable 2 – Phase 2 (To be Agreed Upon with appointed Service Provider – (Feasibly earliest 2019)

8. Acceptance Criteria

The Supplier's services under this Agreement will be considered accepted by the University when:

a. The solution provided is fit for purpose.
b. Requirements have been met and satisfies the need/requirements provided.

9. Risks, Assumptions, Dependencies & Exclusions (RADE)

Risks are uncertain events that may affect the Project objectives should they occur. The Service Provider will effectively manage the risks listed in the Risk Register.**Appendix A**. Comprehensive risk analysis will be performed at the start of the Project and risk management will be performed throughout the life cycle of the Project.

10. Charges and Payment

a. The charges for the Goods and Services are set out in **Annexure 3**.

11. Change Management

The changes made in the project should be noted in the change control log and approved through the change control advisory board. Impact analysis should be conducted thoroughly to depict the change implications in relation to time and charges, if any.

Data migration of the University's knowledge base for all the service request logging tools will need to be planned for, executed and managed effectively through proper and defined change management process.

12. General

a. The Annexures are as follows:

    1. Annexure 1: Scope of Work
        a. Appendix A: Risk Register
    2. Annexure 3: Pricing Schedule

b. The Service Provider shall at all times while this Contract is in force maintain insurance cover satisfactory to the University's insurance brokers, including professional indemnity insurance which adequately insures against all the liabilities imposed by this Contract.

c. The Service Provider shall forward proof of its insurance cover to the University on or about the Start Date and thereafter the terms shall not be altered without the consent of the University. Proof of payment of premium for the policy shall be furnished annually to the University.

d. Clause 13 of the Standard Agreement is amended as follows:

    1. The University has insured itself against the acts and omissions of persons acting on its behalf and its students and staff are insured during the course and scope of the University's business.

    2. The Parties' maximum liability will be limited, whether for a single or multiple events, to the extent of their respective insurance cover herein.

e. Notwithstanding the date of signature of this Agreement, the Agreement commences on the Start Date.

f. The Service Provider shall access the University's precincts and perform work associated with the contract in accordance with the University's specification for Access to and performing works and services on the University's Precincts as set out in **Annexure 3**.

13. Project Plan

ICT to provide a phased implementation plan as per the ITIL processes mentioned below:

Service Request Management

Service Level Management

Service Catalogue

Incident Management

Problem Management

Change Management

Release and Deployment Management

Configuration Management

14. Number of estimated users as per the requirements for each department

Title	Number of contact users	Number of non-contact users	Web based users
Wits ICT Senior Manager – Service Delivery	385	Wits community	Wits community (Otter)
Wits Library Systems – Manager	10 (Licensed)	137 (Supported)	79(Zendesk)
SENC – Call Centre Manager	7 (Licensed)	Wits community	Unlimited (Zendesk)
Business Intelligence – Head Management Information Unit	15 (Licensed)	Wits community	Unlimited (Zendesk)
Procurement – Manager	5 (Licensed)	Wits community + vendors	5 (Zendesk)
HR Systems Manager	They fall under Service Delivery license	Wits community	Wits community (Otter) system)
FIMS – Senior Manager Info Management	They fall under Service Delivery license	Wits community	Wits community (Heat system)
AISU – Head of AISU	Open source	Open source	Open source (Redmine)
Wits ICT Senior Manager BRM	They fall under Service Delivery license	Wits community	Wits community
Wits ICT Senior Manager BAS	They fall under Service Delivery license	Wits community	Wits community
Director Services, Services	-	Wits community	Archibus
Deputy Director, Property & Infrastructure Management	-	Wits community	Archibus
Deputy Director Protection Services, Protection Services	-	Wits community	
Technical Security Solutions Manager, Protection Services	-	Wits community	Otter
Director, Campus Housing And Residence Life	-	Wits community	Archibus
Wits ICT Senior Manager Governance	They fall under Service Delivery license	Wits community	Wits community