TABLE OF CONTENTS

1 GLOSSARY

The following abbreviations and terms are used in this document: -

Term / Abbreviation	Meaning
Wits	The University of the Witwatersrand Johannesburg.
East Campus	The University of the Witwatersrand Johannesburg – East Campus Braamfontein.
West Campus	The University of the Witwatersrand Johannesburg – West Campus Braamfontein

2 INTRODUCTION

2.1 Problem Statement: -

The University's current backup and disaster recovery infrastructure relies on legacy tape-based technology and outdated software, specifically IBM Storage Protect, which has been unsupported for the past four years. This system presents significant operational and security risks, including:

2.1.1 Hardware Obsolescence: The existing tape hardware is over 20 years old and prone to failure, risking critical data loss.

2.1.2 Software Support Expiration: The IBM Storage Protect software is no longer supported, rendering it vulnerable to security threats and incompatible with modern operating systems and virtualization platforms.

2.1.3 Limited Recovery Capabilities: The current system primarily supports file-level backups, making full server recovery complex and time-consuming. It lacks support for virtual machine (VM) image backups, which are essential for our virtualized environment.

2.1.4 Inadequate Cyber and Disaster Recovery: The absence of a dedicated DR tape infrastructure makes disaster recovery complex and time-consuming, potentially leading to significant business disruption.

2.1.5 Insufficient Data Retention: The current 30-day data retention period does not meet the organization's evolving compliance and business requirements.

2.1.6 Security Vulnerabilities: The unsupported system is susceptible to security breaches and data compromises.

Therefore, the organization requires a modern, robust, and scalable backup, cyber and recovery solution to mitigate these risks and ensure business continuity.

2.2 Key Objectives

The organization seeks to procure a comprehensive backup and disaster and cyber recovery solution that achieves the following key objectives:

2.2.1 Enhanced Data Protection: Implement a reliable and resilient backup solution that minimizes the risk of data loss and corruption.

2.2.2 Rapid Recovery Capabilities: Ensure rapid and efficient recovery of critical systems and data, including full VM image backups, to minimize downtime.

2.2.3 Improved Cyber and Disaster Recovery Preparedness: Establish a robust and automated recovery solution that enables seamless recovery in the event of a disaster or cyber-attack.

2.2.4 Extended Data Retention: Implement a flexible and scalable data retention policy that meets the organization's regulatory and business requirements.

2.2.5 Seamless Integration: Ensure seamless integration with existing infrastructure, including Oracle Cloud, Office 365, Google Workspace and on-premises systems.

2.2.6 Enhanced Security: Implement robust security measures, including encryption and access controls, to protect sensitive data.

2.2.7 Cost Optimization: Achieve a cost-effective solution that optimizes the total cost of ownership (TCO) for backup and Recovery.

2.2.8 Dual Data Storage: Ensure backup data is stored in at least two geographically distinct physical locations.

2.2.9 Simplified Management: Provide a centralized and user-friendly management interface for simplified administration and monitoring.

2.2.10 Compliance Adherence: Ensure the solution complies with all relevant data protection regulations, including POPIA and or GDPR.

3 RESPONSIBILITIES AND DELIVERABLES

This section covers all areas of responsibility and deliverables required from the Backup and recovery implementation.

3.1 Wits Deliverables

3.1.1 Requirements:

3.1.1.1 Documentation of current infrastructure, applications, and data.

3.1.1.2 Specific Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for each system.

3.1.1.3 Data retention policies and compliance requirements.

3.1.1.4 Detailed security requirements.

3.1.1.5 Office 365 and Oracle Cloud backup requirements.

3.1.1.6 Recovery testing procedures.

3.1.2 Access Provisioning:

3.1.2.1 Providing necessary access to on-premises systems, virtual environments, and cloud platforms for the supplier.

3.1.2.2 Granting appropriate permissions for backup and recovery operations.

3.1.3 Network Configuration:

3.1.3.1 Ensuring adequate network bandwidth and connectivity for data transfer.

3.1.3.2 Configuring firewalls and network security devices as needed.

3.1.4 Environment Preparation:

3.1.4.1 Preparing the on-premises environment for the new backup hardware/software (if applicable).

3.1.4.2 Ensuring compatibility of existing systems.

3.1.5 Data Validation:

3.1.5.1 Participating in data validation and testing during and after the migration.

3.1.5.2 Validating the integrity of backed-up data.

3.1.6 User Acceptance Testing (UAT):

3.1.6.1 Conducting UAT to ensure the solution meets the organization's requirements.

3.1.6.2 Providing feedback and sign-off on the implemented solution.

3.1.7 Training & Documentation:

3.1.7.1 Ensuring IT staff attend supplier-provided training.

3.1.7.2 Reviewing and utilizing supplier-provided documentation.

3.1.8 Recovery Testing Participation:

3.1.8.1 Participating in and validating Recovery testing.

3.1.9 Ongoing Management:

3.1.9.1 Ongoing management of the backup system once implemented.

3.2 SUPPLIER DELIVERABLES: -

3.2.1 The tenderer / supplier is to make provision for: -

3.2.2 **Solution Design & Architecture**:

3.2.2.1 Detailed design and architecture of the proposed backup and DR and cyber recovery solution.

3.2.2.2 Specification of hardware, software including licenses, and cloud resources.

3.2.2.3 Integration plan for Oracle Cloud, Office 365, and on-premises systems.

3.2.3 **Software & Hardware Provisioning**:

3.2.3.1 Provisioning and installation of backup software and hardware (if applicable).

3.2.3.2 Configuration of cloud storage and recovery resources.

3.2.4 **Data Migration & Configuration**:

3.2.4.1 Data migration from the existing system to the new system.

3.2.4.2 Configuration of backup schedules, retention policies, and security settings.

3.2.5 **Integration & Testing**:

3.2.5.1 Integration of the backup solution with existing systems.

3.2.5.2 Unit testing, integration testing, and performance testing.

3.2.6 **Documentation**:

3.2.6.1 Comprehensive documentation, including installation guides, user manuals, and troubleshooting procedures.

3.2.6.2 Implementation and configuration documentation

3.2.6.3 Recovery run books.

3.2.7 **Training:**

3.2.7.1 Training for IT staff on the operation and management of the backup system.

3.2.7.2 Recovery testing training.

3.2.8 **Project Management:**

3.2.8.1 Project plan, regular status updates, and risk management.

3.2.8.2 Change management.

3.2.9 **Recovery Implementation:**

3.2.9.1 Configuration and implementation of the cloud-based recovery solution.

3.2.9.2 Recovery testing and validation.

3.2.10 **Support:**

3.2.10.1 Ongoing support of the backup system.

3.2.10.2 Service Level Agreements (SLAs) for support response times.

3.2.11 **Security Implementation:**

3.2.11.1 Implementation of security best practices, and configuration of security features.

3.2.11.2 Compliance documentation.

3.2.12 **Reporting:**

3.2.12.1 Configure reporting and dashboard on backup success rates, storage utilization, and other relevant metrics.

4 REQUIREMENTS

4.1 Scope of Backup and Recovery Solution

4.1.1 On-Premises Systems:

4.1.1.1 The solution must provide comprehensive backup and recovery capabilities for minimum 500TB of on-premises data.

4.1.1.2 Supported operating systems: Windows Server, Linux Server including filesystem snapshot support.

4.1.1.3 Virtualization platforms: Hyper-V cluster (primary), VMware, KVM.

4.1.1.4 Integration with existing Tivoli Storage Manager (TSM) for potential migration.

4.1.2 Oracle Cloud Infrastructure (OCI):

4.1.2.1 The solution must provide robust backup and recovery for a minimum 250TB of OCI data.

4.1.2.2 Supported OCI services: Linux/Windows Virtual Machines, Oracle Base/Autonomous Databases, Object Storage.

4.1.2.3 Integration with OCI native backup utilities and ability to enhance them.

4.1.3 Microsoft 365 (M365):

4.1.3.1 The solution must provide robust archiving and long-term retention capabilities independent of the native retention, licensing and recycle bin functionality for minimum 400TB of M365 data.

4.1.3.2 Supported M365 services: Exchange Online, SharePoint Online, OneDrive for Business, Teams (including chat messages and channel files).

4.1.3.3 Granular item-level recovery and search functionality.

4.1.4 Google Workspace:

4.1.4.1 The solution must provide robust archiving and long-term retention capabilities for minimum 3000TB of Google Workspace data.

4.1.4.2 Supported Google Workspace services: Gmail, Google Drive, Shared Drives, Google Meet recordings.

4.1.4.3 Granular item-level recovery and search functionality.

4.2 Functional Requirements

4.2.1 Backup Capabilities:

4.2.1.1 Agent-based and agentless backup options.

4.2.1.2 Incremental, differential, and full backup capabilities.

4.2.1.3 Application-aware backups for databases and critical applications.

4.2.1.4 Consistent backup of virtual machines, regardless of hypervisor.

4.2.1.5 Automated backup scheduling and policy management.

4.2.1.6 Data deduplication and compression to optimize storage utilization.

4.2.1.7 Encryption of data in transit and at rest.

4.2.1.8 Ability to backup to cloud based storage.

4.2.2 Recovery Capabilities:

4.2.2.1 Rapid and reliable restoration of individual files, folders, applications, and entire systems.

4.2.2.2 Granular recovery of M365 and Google Workspace data, ideally without requiring user account recreation.

4.2.2.3 Ability to restore on-premises systems to cloud environments (e.g., Hyper-V VMs to Azure, AWS or OCI).

4.2.2.4 Ability to restore cloud-based systems to on premise locations.

4.2.2.5 Bare-metal recovery for physical servers.

4.2.2.6 Virtual machine instant recovery.

4.2.2.7 Automated disaster recovery orchestration.

4.2.3 Archiving Requirements (e.g. M365 and Google Workspace):

4.2.3.1 Long-term retention of data in compliance with regulatory requirements.

4.2.3.2 Legal hold functionality.

4.2.3.3 Advanced search and eDiscovery capabilities.

4.2.3.4 Immutable storage options.

4.2.4 **Storage Requirements:**

4.2.4.1 Data must be stored in two geographically separate physical locations for redundancy and disaster and cyber recovery.

4.2.4.2 Scalable storage architecture to accommodate future growth.

4.2.4.3 Support for various storage media (e.g., disk, tape, cloud).

4.2.5 **Reporting and Monitoring:**

4.2.5.1 Comprehensive reporting on backup success rates, storage utilization, and other relevant metrics.

4.2.5.2 Real-time monitoring of backup and recovery operations (Dashboard) .

4.2.5.3 Alerting and notification for backup failures and other critical events.

4.2.6 **Ransomware Protection**

4.2.6.1 **Immutable Storage:**

4.2.6.1.1 The solution must provide immutable storage options to prevent ransomware from encrypting or deleting backup data.

4.2.6.1.2 Implement air-gapped or offline backup options for critical data.

4.2.6.2 **Anomaly Detection:**

4.2.6.2.1 The solution must include anomaly detection capabilities to identify unusual backup activity that may indicate a ransomware attack.

4.2.6.2.2 Implement real-time monitoring for suspicious file modifications, encryption attempts, or rapid data growth.

4.2.6.3 **Ransomware Scanning:**

4.2.6.3.1 The solution must integrate with or include built-in ransomware scanning capabilities to detect and remove malicious files from backups.

4.2.6.3.2 Implement regular, automated scans of backup data.

4.2.6.4 **Rapid Recovery from Ransomware:**

4.2.6.4.1 The solution must enable rapid and granular recovery of data from clean backup copies in the event of a ransomware attack.

4.2.6.4.2 Implement automated recovery workflows to minimize downtime and data loss.

4.2.6.4.3 Provide the ability to rapidly create an isolated recovery environment, to test the recovered data, before placing it back into production.

4.2.6.5 **Incident Response and Recovery Planning:**

4.2.6.5.1 The supplier must provide guidance and support for developing and implementing a ransomware incident response and recovery plan.

4.2.6.5.2 Include detailed procedures for identifying, isolating, and recovering from ransomware attacks.

4.2.6.5.3 Provide documentation on how to perform a clean recovery.

4.2.7 **Data Validation:**

4.2.7.1 The solution must provide tools to validate the integrity of backup data, to ensure that it has not been tampered with.

4.2.7.2 Automatic validation of backup data after the backup process has been completed.

4.3 Non-Functional Requirements

4.3.1 **3.1 Performance:**

4.3.1.1 Minimization of backup and recovery windows.

4.3.1.2 High throughput and low latency.

4.3.1.3 Scalability to handle large data volumes and high transaction rates.

4.3.2 **Security:**

4.3.2.1 Compliance with industry security standards and best practices.

4.3.2.2 Role-based access control.

4.3.2.3 Auditing and logging of all backup and recovery activities.

4.3.2.4 Implement strong access controls, multi-factor authentication, and encryption.

4.3.2.5 The solution must have the ability to restrict or limit access to the backup system, from the production network.

4.3.3 **Reliability and Availability:**

4.3.3.1 High availability of the backup and recovery infrastructure.

4.3.3.2 Robust error handling and fault tolerance.

4.3.4 **Manageability:**

4.3.4.1 Centralized management console.

4.3.4.2 Automation of routine tasks.

4.3.4.3 User-friendly interface.

4.3.5 **Compliance:**

4.3.5.1 Compliance with relevant data privacy regulations (e.g., GDPR, POPIA).

4.3.5.2 Ability to generate compliance reports.

5 SERVICES: -

Tenderers are required to provide a comprehensive suite of services encompassing the entire lifecycle of the backup and disaster recovery solution. These services must include, but are not limited to:

5.1 Solution Design and Architecture:

5.1.1 Detailed design and architecture of the proposed backup and DR solution, including a clear explanation of how the solution addresses the organization's specific requirements.

5.1.2 Specification of all hardware, software, and cloud resources required for the implementation.

5.1.3 A comprehensive integration plan outlining how the solution will integrate with Oracle Cloud, Microsoft 365, Google Workspace, and on-premises systems.

5.2 Implementation and Deployment:

5.2.1 Provisioning and installation of all necessary backup software and hardware (if applicable).

5.2.2 Configuration of cloud storage and recovery resources, including the setup of geographically separate storage locations.

5.2.3 Data migration from the existing Tivoli Storage Manager and other existing systems to the new backup solution.

5.2.4 Configuration of backup schedules, retention policies, security settings, and ransomware protection measures.

5.2.5 Integration of the backup solution with existing systems, including application-aware backups.

5.2.6 Configuration and implementation of the cloud-based recovery solution, including the ability to restore on-premises systems to the cloud and vice versa.

5.3 Testing and Validation:

5.3.1 Unit testing, integration testing, and performance testing of the backup solution.

5.3.2 Recovery testing and validation, including simulated disaster recovery scenarios and ransomware recovery tests.

5.3.3 Recovery testing training for IT staff.

5.4 Project Management and Reporting:

5.4.1 A detailed project plan with clear milestones and timelines.

5.4.2 Regular status updates and risk management reports.

5.4.3 Change management procedures to ensure smooth transitions and minimal disruption.

5.4.4 Configure reporting on backup success rates, storage utilization, and other relevant metrics.

5.5 Security and Compliance:

5.5.1 Implementation of security best practices, including strong access controls, encryption, and multi-factor authentication.

5.5.2 Configuration of security features to protect against unauthorized access and ransomware attacks.

5.5.3 Provision of compliance documentation to demonstrate adherence to relevant data privacy regulations.

5.6 Post-Handover Support:

5.6.1 The tenderer must provide a defined period of post-handover support to assist Wits IT staff with any questions or issues that may arise.

5.6.2 The tenderer must define the duration and scope of post-handover support in their proposal.

5.6.3 The tenderer must provide escalation paths for support.

5.7 Ongoing Support and Maintenance:

5.7.1 Ongoing support of the backup system, including troubleshooting, updates, and maintenance.

5.7.2 Clearly defined Service Level Agreements (SLAs) for support response times and system availability.

5.8 Project Team Portfolios.

5.8.1 Accounts Manager

To manage all commercial and accounting matters of the project, for example, quotations, variation order, ordering equipment and licensing, dealing with procurement matters, account queries and escalations where required.

5.8.1.1 **Project Manager**

A suitably qualified project manager that has both project management experience and certification to perform this function. The Project Manager will be responsible for the overall management of the supplier's implementation of the project in addition to hand-over processes of the solution to both the supplier's services department and the Wits Projects Team or other Wits assigned personnel. These tasks need to include the sign-off of project and payment milestones as required and agreed between both the supplier and Wits in conjunction with an approved implementation plan.

5.8.1.2 **Lead Engineer**

A qualified person that is responsible for all technical aspects of the total project..

5.8.2 **Tenderer CV's:**

CV's are required for all project team and maintenance members that are to participate in the project for both on and off-site activities. The CV's would need to include: -

- Qualifications and certifications that include copies of their qualifications and any other relevant supporting documentation.
- Experience summary detailing key deployments and personal references where available.
- Duration of their experience in the ICT industry.

5.9 TOTAL SOLUTION PROJECT PLAN

The tenderer is to provide a project plan that integrates with their implementation plan and covers expected timescales on important tasks, critical- paths, and milestone events. Note the how these tasks are performed is not required in the Project Plan as these are to be catered for in the Implementation Plan – refer point 5.4 below. The listed tasks that are of importance for the project to proceed will need to be included, for example "testing and acceptance of functional requirement". The plan is to be submitted in a separate schedule and named "Schedule 5.8 Project Plan.

5.10 TOTAL SOLUTION IMPLEMENTATION PLAN: -

The tenderer is to provide comprehensive details and compliance to all aspects of their Implementation plan in their submission document "Schedule 5.9 Implementation Plan". The plan is to supply details on all activities and time frames on the processes that are to be followed. The

tenderer is to be clear on the importance of this requirement as the implementation plan will be extensively analysed and scored by the Wits Technical Evaluation Committee on both the plans detail and its methodologies.

5.10.1 **Implementation Plan Milestones**

The implementation plan is to enable all aspects of the total solution and is to cover the following topics as a minimum: -

- Initiation of the Project
- Site Preparation
- Testing Processes
- Initial Installation
- Proof of Technology
- Installation and Commissioning of Services
- Final Design
- Signoffs
- Deployment
- Switchover / Cut-Over
- Hand over to Maintenance processes.

5.10.2 **Information**

The information which follows is information that is valuable in assisting the tenderer to present their own plans and recommended tasks where appropriate.

5.10.2.1 **Data centre facilities**

5.10.2.1.1 Wits operates across two main datacentres (East and West Campus) roughly 1 km apart. Though not enough to act as DR the second datacentre can be used for high availability

5.10.2.1.2 There are 100 Gb ethernet links joining the two datacentres on a stretched network.

5.10.2.1.3 There are Fibre Channel links available between the datacentres, but the Fibre Channel switches are out of date and unsupported.

5.10.2.1.4 Network points: Both datacentres provide 10Gb Fibre and copper for server connectivity.

5.10.2.1.5 Internet access: 10 Gb links provided by Tenet with failover capability between the two datacentres.

5.10.2.1.6 Cloud access: 1Gb Fast Connect to Oracle Cloud

5.11 TRAINING AND SKILLS TRANSFER

5.11.1 OEM Training

5.11.1.1 OEM training and certification path for staff members on the operation and management of the backup system, including recovery procedures.

5.11.2 Knowledge Transfer:

5.11.2.1 The tenderer must provide comprehensive knowledge transfer to Wits IT staff throughout the project lifecycle, culminating in a formal handover.

5.11.2.2 This includes detailed explanations of the solution's architecture, configuration, operation, and troubleshooting procedures.

5.11.2.3 The tenderer must provide access to all relevant documentation, including design documents, configuration files, and operating procedures.

5.11.2.4 The tenderer must provide detailed documentation of all customisations.

5.11.3 Handover Documentation:

5.11.3.1 The tenderer must deliver a comprehensive handover package, including:

5.11.3.1.1 As-built documentation detailing the final configuration of the backup and recovery solution. This documentation must encompass all aspects of the proposed solution, including system architecture, installation procedures, configuration settings, integration details, and any customization performed

5.11.3.1.2 Detailed operating procedures and maintenance guides.

5.11.3.1.3 Troubleshooting guides and known issue logs.

5.11.3.1.4 A complete inventory of all hardware and software components.

5.11.3.1.5 All licensing information.

5.11.3.1.6 All access credentials.

5.11.3.2 All documentation must be provided in an electronic format.

5.11.4 **Handover Training:**

5.11.4.1 The tenderer must conduct dedicated handover training sessions for Wits IT staff, covering all aspects of the backup and recovery solution.

5.11.4.2 Training must be tailored to the specific roles and responsibilities of Wits IT staff.

5.11.4.3 Training must include hands-on exercises and practical scenarios.

5.11.4.4 The tenderer must provide training material that can be used for future training sessions.

5.12 SERVICE LEVEL AGREEMENT

5.12.1 **Commencement and Duration.**

5.12.1.1 The commencement of the services for all aspects of the total solution shall take effect from the date of the official hand-over to both Wits and the tenderer's services division.

5.12.1.2 All terms and conditions of contract shall be in accordance with the Wits contract with the supplier.

5.12.2 **Service Level Criteria**

5.12.2.1 **Level 1 – Top Priority**

5.12.2.1.1 Interpretation – Any area that has a major impact to Wits Business or that can run the risk of loss of crucial data or service availability.

5.12.2.1.2 Reporting facility – 24/7/365

5.12.2.1.3 Response and commencement time – attendance to the repair within 2 Hours. This can be performed remotely on or off-site.

5.12.2.2 **Level 2 – Medium Priority**

5.12.2.2.1 Interpretation – Any area that is strategic to the business that has partial services

5.12.2.2.2 Reporting facility – Normal office hours.

5.12.2.2.3 Response and commencement time – attendance to the repair within 4 Business Hours. This can be performed remotely on or off-site.

5.12.2.3 **Level 3 – Low Priority**

5.12.2.3.1 Interpretation – Any area that has a minimal impact to the business.

5.12.2.3.2 Reporting facility – Normal office hours,

5.12.2.3.3 Response and commencement time – attendance to the repair – next business day Business Hours. This can be performed remotely on or off-site.

5.12.2.4 **Level 4 – Minor events or non-urgent configuration changes**

5.12.2.4.1 Interpretation – Any area that has non or negligible impact to the business.

5.12.2.4.2 Reporting facility – Normal office hours,

5.12.2.4.3 Response and commencement time – attendance to the repair or change – 5 business days. This can be performed remotely on or off-site.