



APPENDIX B-1(SERVICE SPECIFICATION) BACK UP AS A SERVICE (“BaaS”)

Table of Contents

1. Introduction.....	4
2. Abbreviations.....	4
3. Definitions.....	5
4. Scope of Work / Business Requirements – Front End	7
4.1. Compliance of the Backup Solution to Applicable Standards and Governance.....	7
4.2. Enabling IT Business Continuity	7
4.3. Backup Policy: Frequency, Retention and Archiving.....	8
4.4. Periodic Backup Restore Testing	9
4.5. Data Backup and Storage Infrastructure Technology	9
4.6. Security and Encryption.....	10
4.7. Monitoring and Reporting	10
4.8. Automation and Backup Failure Prevention.....	11
4.9. Scalability.....	11
5. Facts and Figures – Backend Systems.....	11
6. Scope of Work / Business Requirements – Endpoint Backup	11
6.1. Device Coverage.....	11
6.2. Data Types.....	11
6.3. Backup Frequency	12
6.4. Storage and Location	12
6.5. Recovery Process	12
6.6. Access Control	13
6.7. Retention Policies.....	13
6.8. Monitoring and Reporting	13
7. Service Level Agreement Requirements.....	14
7.1. Front-End Server.....	14
7.2. Endpoint Devices	14
8. Inclusions	15
9. Exclusions	15
10. Training and Transfer of Skills	15
10.1. End-User Training	16
10.2. IT Support and End User Computing Teams	16
10.3. Backup Administrators / Infrastructure Teams	16
10.4. Disaster Recovery and Business Continuity Teams	17
10.5. Security and Compliance Teams.....	17
11. Professional Services for BaaS – Non-Committal	17
11.1. Assessment and Planning	17
11.2. Solution Design	17
11.3. Implementation and Configuration.....	18
11.4. Data Migration and Seeding	18
11.5. Testing and Validation	18

11.6. Training and Knowledge Transfer.....	18
11.7. Ongoing Support and Optimisation.....	18
11.8. Compliance and Audit Support.....	19
12. Professional Services Roles for BaaS	19
12.1. Backup Solutions Architect.....	19
12.2. Backup Implementation Engineer.....	19
12.3. Data Migration Specialist.....	19
12.4. Disaster Recovery Consultant	19
12.5. Security and Compliance Analyst.....	20
12.6. Monitoring and Reporting Specialist	20
12.7. Training and Enablement Lead.....	20
12.8. Project Manager	20
12.9. Support and Optimisation Engineer	20
13. Responsibility Matrix (RACI).....	20

1. Introduction

Backup as a Service (BaaS) is a managed service through which the service provider is expected to deliver data backup and recovery capabilities for Eskom data hosted across on-premises, cloud, and hybrid IT environments, including servers, applications, databases, endpoints, and related systems.

Although data protection solutions are deployed to safeguard Eskom information assets, backup remains a critical last line of defence, enabling the organisation to recover from data loss caused by malicious deletion, storage subsystem failure, system corruption, or any other incident that may result in business interruption.

Backups also provide Eskom with the flexibility to migrate IT operations from the primary site and re-establish services at a recovery site. This is enabled by the solution's inherent capability to replicate data to an alternate location, where it can be restored into the disaster recovery environment when required.

As backup does not address all disaster recovery scenarios, its role within the overall DR strategy will be determined by the Disaster Recovery or IT Business Continuity function, informed by the outcomes of the Business Impact Analysis.

The service provider is therefore required to propose a fit-for-purpose and flexible BaaS solution that aligns with Eskom's disaster recovery requirements for each application recorded in the Eskom CMDB. The BaaS solution is expected to support the predefined outcomes of the Business Impact Analysis, including the applicable Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), and the role that backup and restore capabilities will play in the event of an IT disaster.

2. Abbreviations

Abbreviation	Explanation
AES	Advanced Encryption Standard
AIR	Automatic Image Replication
BaaS	Backup as a Service
CMDB	Configuration Management Database
D2D2C	Disk-to-Disk-to-Cloud
D2T	Disk-to-Tape
DMS	Document Management System
DR	Disaster Recovery
EUC	End User Computing
EUS	End User Support
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
ICT	Information and Communication Technology
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
ITOM	IT Operations Management

Abbreviation	Explanation
MFA	Multi-Factor Authentication
OST	Open Storage Technology
PC	Personal Computer
POPIA	Protection of Personal Information Act
RACI	Responsible, Accountable, Consulted, Informed
RBAC	Role-Based Access Control
RDBMS	Relational Database Management System
RFP	Request for Proposal
RPO	Recovery Point Objective
RTO	Recovery Time Objective
S3	Simple Storage Service
SLA	Service Level Agreement
SOW	Scope of Work
STU	Storage Unit
VTL	Virtual Tape Library

3. Definitions

Term	Definition and Explanation
Backup as a Service	A managed service through which the Service Provider delivers backup, replication, recovery, monitoring and reporting capabilities for Eskom data hosted across on-premises, cloud and hybrid environments.
Backup Data	A protected copy of Eskom business-related data created and retained in accordance with the applicable backup schedules, retention periods and recovery requirements defined in this document.
Backup Window	The defined period during which scheduled backup jobs must run and complete, currently referenced as 18:00 to 06:00 for daily backup processing.
Business Impact Analysis	The assessment used to determine the criticality of applications and services, including the applicable recovery requirements, recovery priorities, Recovery Time Objectives and Recovery Point Objectives.
Cloud Backup	Backup storage hosted in a cloud environment and used for replication, offsite retention, long-term archival or protection of workloads hosted on Hyperscalers platforms.

Term	Definition and Explanation
Configuration Management Database	The authoritative repository of configuration items and application records used to compare backup coverage and identify systems or devices that are not protected by the backup solution.
Deduplication	A storage optimisation process that eliminates duplicate data blocks to reduce storage consumption and improve backup efficiency.
Disaster Recovery	The capability, process and supporting environment used to restore Eskom systems, services and data following a disruptive incident or disaster.
Endpoint Backup	The backup of Eskom business-related data residing on Eskom-issued laptops or desktop computers, subject to the scope, frequency, access control and retention rules defined in this document.
Encryption	The protection of data by converting it into a secure format that can only be accessed by authorised parties, including encryption of data at rest and in transit.
Offsite Storage	A storage location physically or logically separated from the primary production site, used to retain backup copies for resilience, recovery and compliance purposes.
Recovery Point Objective	The maximum acceptable amount of data loss measured in time, used to determine the required backup frequency and replication approach for a workload.
Recovery Time Objective	The maximum acceptable time required to restore a system, service or data set following an incident or disruption.
Replication	The transfer or synchronisation of backup data from one storage location to another, including to a disaster recovery site, offsite repository or cloud backup environment.
Restore	The process of recovering data, systems or services from a backup copy to a usable state following deletion, corruption, system failure, testing or another recovery requirement.
Retention Period	The period for which a backup copy must be retained before it expires or is purged in accordance with Eskom's backup, archival and compliance requirements.

Term	Definition and Explanation
Service Level Agreement	The agreed measurable service performance requirement, including backup success, replication success, restore success, backup testing and reporting obligations.

4. Scope of Work / Business Requirements – Front End

4.1. Compliance of the Backup Solution to Applicable Standards and Governance

The proposed Backup as a Service (BaaS) solution must demonstrate full compliance with **ISO/IEC 27031:2025**, which provides a framework for ensuring ICT readiness to support business continuity. This includes the ability to prevent, respond to, and recover from ICT-related disruptions in alignment with broader organizational resilience objectives.

In addition, the solution must adhere to all applicable South African statutory and regulatory requirements governing data protection and privacy. This includes, but is not limited to:

- The Protection of Personal Information Act (POPIA) – ensuring lawful processing, storage, and transmission of personal data.
- Data Sovereignty Requirements – ensuring that sensitive and regulated data is stored and processed within South African borders, unless explicitly permitted otherwise.
- Any other sector-specific or national regulations relevant to data governance, cybersecurity, and digital continuity.
- The BaaS provider must ensure that all data handling practices, including backup, replication, and archival, are aligned with these legal and regulatory frameworks to mitigate compliance risks and support Eskom's governance objectives.

4.2. Enabling IT Business Continuity

Backup will remain the primary recovery option for lost data where the required recovery outcomes fall within the capability of the backup solution. Where workloads require more aggressive RTO or RPO targets than the BaaS solution can support, Eskom may implement alternative or supplementary continuity strategies.

4.2.1. BaaS – Data Backup (D2D2C)

As part of this service, the BaaS vendor shall provide Eskom with the following service offerings, based on the principle of maintaining three backup copies across different media, with one monthly backup copy stored offsite:

Backup Copy	Frequency	Media
Copy 1: Backup of Eskom Data on daily basis at Eskom primary production site	Daily (18:00 to 06:00)	Disk
Copy 2: Replication of daily Backup Data to a designated Disaster Recovery site or Cloud Backup in the case of the Regional Sites, via a dedicated link to be provided by the vendor as an option.	Daily after a Successful Backup (06:00 to 17:59)	Disk
Copy 3: Monthly Backup replicated to Cloud Backup for long term retention or Backup archiving for compliance via a dedicated link provided by the vendor as an option.	Monthly	Disk

4.2.2. BaaS – Data Backup (D2T)

Where a new network link or network upgrade cannot be implemented to enable backup replication, the service provider shall deploy a tape-based backup solution or Virtual Tape Library (VTL) and establish an agreement with a data management facility for the weekly collection and secure offsite storage of tapes.

Backup Copy	Frequency	Media
Copy 1: Backup of Eskom Data on daily basis at Eskom primary production site and retained for 4 weeks	Daily (18:00 to 06:00)	Disk
Copy 2: Write Off Data to Tape media for collection by Data Management service for long term retention	Monthly	Tape

4.3. Backup Policy: Frequency, Retention and Archiving

The BaaS solution shall comply with the backup policy outlined below and with the Eskom Data Backup Standard, as updated from time to time, unless otherwise formally approved by Eskom.

This policy defines the frequency, retention periods, storage media, backup locations, and replication cadence to ensure data availability, compliance, and long-term preservation.

Backup Type	Retention Period	Media	Site	Replication Frequency
Daily Incremental	4 Weeks	Disk	Prod and DR	Daily, post-backup window
Weekly Full	4 Weeks	Disk		
Monthly Full	12 Months	Cloud	Offsite	
Yearly Backup	7 Years	Cloud	Offsite	
Archive Logs	1 Week	Disk	Prod and DR	

This policy ensures a layered and resilient backup strategy that supports both operational recovery and long-term archival, while meeting Eskom's compliance and governance requirements.

4.4. Periodic Backup Restore Testing

The BaaS vendor shall lead and coordinate periodic backup restore testing activities by engaging the IaaS vendor and Eskom DR teams to validate backup integrity, recoverability, recovery performance and audit readiness.

Where feasible, the vendor should provide automated backup validation to verify backup integrity, simulate restore scenarios and generate audit-ready reports without unnecessary manual intervention.

4.5. Data Backup and Storage Infrastructure Technology

Eskom requires a scalable backup infrastructure that supports high-performance data protection, efficient storage utilisation, deduplication, compression, replication and recovery across on-premises, regional and cloud-hosted workloads. Vendors may propose equivalent or improved technologies, provided that the solution meets Eskom's performance, resilience, security and cost-efficiency requirements.

4.5.1. Primary Backup Storage Unit (STU)

- Must support Open Storage Technology (OST) to enable seamless integration with backup software.
- Should facilitate Automatic Image Replication (AIR) across sites for enhanced data resilience.
- Must deliver a minimum deduplication and compression ratio of 10:1, optimised to complete backup operations within the designated backup window of 18:00 to 06:00.

4.5.2. Tape-Based Offsite Backup for Bandwidth-Constrained Sites

- Recommended for sites with limited connectivity where cloud-based deduplication is not feasible.
- The solution must include:
 - A tape library and connectivity capable of supporting the required backup and restore performance.
 - Cleaning tapes and tape media for operational maintenance.
 - Manual or automated tape handling (robotic arm preferred); if unavailable, the vendor must provide tape rotation services.
 - Secure transportation to an offsite tape storage facility located at least 25 km from the originating site, with the ability to deliver tapes to impacted sites within 4 hours, where operationally feasible and commercially agreed.

4.5.3. Cloud Backup Hosting for Hyperscalers Workloads

- The cloud backup solution must be S3-compatible, enabling seamless migration of backup data between cloud and on-premises environments.
- This ensures interoperability across multiple Hyperscalers platforms and supports Eskom's hybrid cloud strategy.

4.6. Security and Encryption

The BaaS solution must incorporate appropriate data protection mechanisms to ensure the confidentiality, integrity, availability and recoverability of backup data.

- Encryption: End-to-end encryption of data both in transit and at rest, using industry-standard protocols (e.g., AES-256).
- Deduplication: Efficient data deduplication to reduce storage footprint and enhance performance.
- Replication: Secure replication across multiple sites or media to ensure redundancy and resilience.
- Ransomware Protection: The solution must include capabilities to detect, prevent, and recover from ransomware attacks, ensuring backup data remains uncompromised and recoverable.

4.7. Monitoring and Reporting

The vendor shall utilise the monitoring and reporting capabilities of the backup platform to manage day-to-day operations, integrate with Eskom's IT Operations Management tools where required, and provide coverage reports that can be compared against the CMDB to identify backup gaps.

4.8. Automation and Backup Failure Prevention

Where applicable, the backup solution must proactively identify potential backup failures, alert the responsible backup engineer and, where feasible, initiate predefined remediation before the risk becomes an operational issue. This may include integration with RDBMS and application-layer tools.

4.9. Scalability

The BaaS infrastructure must be scalable enough to accommodate unexpected data growth and evolving business requirements without disrupting backup operations, while supporting cost-conscious capacity management.

5. Facts and Figures – Backend Systems

Eskom operates a distributed IT environment comprising regional offices across South Africa, supporting functions such as maintenance, customer service and power generation. While most enterprise applications are centralised at the Head Office (Megawatt Park), there are localised workloads at regional sites that require dedicated backup and recovery capabilities.

The current estimated footprint for backup coverage is as follows:

Site	FET
Head Office – Megawatt Park	1800
Regional Offices	450
Cloud – Hyperscalers workloads (estimate)	550

Note: 80% of the above services will be rendered at on-prem or regional offices with elastic cloud capability catering for 20% of the capacity for workloads as determined by the Cloud Centre of Excellence.

6. Scope of Work / Business Requirements – Endpoint Backup

6.1. Device Coverage

Eskom supports a workforce of approximately **42,000 users**, with an estimated **80% to 90%** utilising Eskom-issued desktop or laptop devices. These endpoints are considered critical assets and must be included in the enterprise backup strategy. All data residing on these devices must be protected through:

- Endpoint encryption to ensure data confidentiality and prevent unauthorised access.
- Automated backup to safeguard business-critical information and support recovery in case of device failure, loss, or compromise.

6.2. Data Types

To maintain data integrity and uphold privacy standards, the backup solution must focus exclusively on Eskom business-related data. Through the End User Computing (EUC)

service, a designated folder will be provisioned on each user device. This folder will serve as the authorised repository for Eskom data, including:

- Business documents
- Project files
- Email archives (where applicable)

This approach ensures that personal user data is excluded from the backup scope, in alignment with the principles of data minimisation and fair use under POPIA and other applicable data protection regulations. Eskom will not be obligated to back up any data outside the defined business scope.

6.3. Backup Frequency

Endpoint backups shall be scheduled on a weekly basis, based on the assessment that the rate of data change on user devices is generally low and does not necessitate more frequent backups. To further mitigate the risk of data loss between backup intervals, Eskom users will be encouraged to store all business-related data within designated document management systems (DMS). This approach ensures that critical data is continuously protected and centrally managed, reducing reliance on endpoint backups for day-to-day data recovery.

6.4. Storage and Location

All endpoint backup data will be directed to regional backup media deployed across Eskom's regional offices, including the Disaster Recovery (DR) site and Head Office (Megawatt Park). This distributed storage model is designed to:

- Minimise network congestion by keeping backup traffic local to the user's region
- Improve backup and restore performance
- Enhance data locality and compliance

For users who operate in mobile or rotating roles and frequently work from different locations, their backup data will traverse the network to reach their assigned backup media server. These exceptions will be managed through intelligent routing and bandwidth-aware scheduling to minimise impact on network performance.

6.5. Recovery Process

Users must be able to recover data from the designated backup media server with support from the End User Support (EUS) team. Where feasible, and following appropriate training and competency validation, users should be empowered to perform self-service restores for routine recovery scenarios. This approach enhances operational efficiency while maintaining control over more complex or sensitive recovery operations through EUS oversight.

6.6. Access Control

All data residing on endpoint devices is subject to the provisions of the Protection of Personal Information Act (POPIA) and Eskom's internal Information Security policies and protocols. To ensure compliance and safeguard sensitive information, the endpoint backup solution must enforce robust access control mechanisms, including:

- Role-based access controls (RBAC)
- Multi-factor authentication (MFA)
- Encryption of data at rest and in transit
- Audit logging and access monitoring

These controls are essential to prevent unauthorised access to user data and to uphold Eskom's commitment to data privacy and security.

6.7. Retention Policies

User endpoint data shall be backed up on a weekly basis, with each weekly backup consolidated into a monthly backup image. These monthly backups will be retained for a period of 12 months, after which they will be automatically expired and purged in accordance with Eskom's data retention and compliance policies. This retention strategy ensures a balance between data availability, storage efficiency, and regulatory alignment.

6.8. Monitoring and Reporting

The endpoint backup solution must include robust monitoring and reporting capabilities to ensure visibility, accountability, and compliance with service level agreements (SLAs). Key requirements include:

- Coverage Reporting: The system must generate reports that can be cross-referenced with the Configuration Management Database (CMDB) to identify devices that are not currently protected by backup.
- Monthly SLA Reporting: A formal report must be produced on a monthly basis to demonstrate adherence to SLA targets. The expected performance thresholds are:
 - 95% device coverage (i.e., devices enrolled in the backup system)
 - 95% backup success rate for those devices

These reports will serve as evidence of operational effectiveness and will support continuous improvement initiatives within the endpoint backup programme.

7. Service Level Agreement Requirements

7.1. Front-End Server

Eskom defines three service tiers based on the business criticality of the environment. The following SLA metrics apply to all tiers, with performance targets measured and reported as specified:

Measurement	Frequency	Target
Backup Success Rate	Daily	≥ 95% of scheduled backup jobs must complete successfully
Replication Success	Daily	100% of successfully completed backups must be replicated to the designated DR site
Restore Success	On-demand or during DR testing	All successfully backed-up systems selected for restore validation must be restorable
Tape Restore SLA	As required	Backup tapes must be delivered to the impacted site within 4 hours of request, where operationally feasible and commercially agreed
Backup Testing	Quarterly (every 3 to 4 months)	100% of tested backups must pass restore validation

These SLA metrics are critical to ensuring data availability, operational resilience, and compliance with Eskom's business continuity and disaster recovery objectives.

Eskom system classifications should be considered when finalising the solution design and confirming the applicable backup, replication and restore requirements.

7.2. Endpoint Devices

The following SLA metrics apply to endpoint backup services, ensuring consistent data protection and recovery capabilities for Eskom-issued user devices:

Measurement	Frequency	Target
Backup Success Rate	Weekly	≥ 95% of scheduled endpoint backups must complete successfully
Restore Success	On request	All successfully backed-up endpoint devices selected for restore validation must be restorable
Backup Testing	Quarterly (every 3 to 4 months)	100% of tested endpoint backups must pass restore validation

These SLAs are designed to ensure that user data is reliably protected and recoverable, while also supporting Eskom's broader compliance and business continuity objectives.

8. Inclusions

This Scope of Work encompasses all components necessary to ensure the secure, reliable, and compliant backup of Eskom's data assets, regardless of the hosting environment (on-premises, regional, or cloud) or platform (servers, endpoints, or SaaS applications). The scope includes, but is not limited to:

- Backup and recovery software licenses
- Backup infrastructure (e.g., storage units, tape libraries, cloud storage)
- Endpoint backup agents and configurations
- Network connectivity and bandwidth provisioning for replication and restore
- Encryption and security mechanisms
- Monitoring, reporting, and alerting tools
- Integration with ITSM, CMDB, and RDBMS platforms
- Automation and orchestration tools for backup validation and failure prevention
- Professional services for implementation, configuration, and training
- Ongoing support and maintenance

9. Exclusions

The following items are explicitly excluded from the scope of this Backup as a Service (BaaS) engagement:

- Mobile Devices: Backup of smartphones, tablets, and other mobile computing devices is not included.
- Non-Standard Devices: Any device that does not meet the classification of a server, desktop PC, or laptop is excluded from the backup scope.

These exclusions are based on Eskom's current data protection strategy and device classification standards.

10. Training and Transfer of Skills

For a successful implementation and adoption of Backup as a Service (BaaS) at Eskom, training will be essential across multiple user groups. The typical training requirements, aligned with Eskom's operational structure and technical environment, are set out below:

10.1. End-User Training

Audience: Eskom employees using laptops/desktops

Purpose: Ensure users understand how to store data correctly for backup and perform basic restores (if self-service is enabled)

Topics:

- Use of designated folders for business data
- What data is backed up vs. excluded (e.g., personal files)
- How to request a restore or perform self-service recovery
- Data privacy and compliance awareness (POPIA)

10.2. IT Support and End User Computing Teams

Audience: First-line support and desktop engineers

Purpose: Equip support teams to assist users and troubleshoot endpoint backup issues

Topics:

- Endpoint agent installation and configuration
- Monitoring backup status and resolving failures
- Performing assisted restores
- Logging and escalation procedures

10.3. Backup Administrators / Infrastructure Teams

Audience: Backup Managers

Purpose: Manage and monitor the BaaS platform

Topics:

- BaaS platform architecture and components (e.g., STU, OST, AIR)
- Policy configuration (retention, schedules, replication)
- Monitoring dashboards and alerting
- Restore testing and reporting
- Integration with CMDB, ITOM, and RDBMS tools
- Security features (encryption, access control, ransomware protection)

10.4. Disaster Recovery and Business Continuity Teams

Audience: DR coordinators, continuity planners

Purpose: Validate backup readiness and support DR testing

Topics:

- Restore validation procedures
- DR test planning and execution
- SLA compliance tracking
- Coordination with IaaS and cloud teams

10.5. Security and Compliance Teams

Audience: Information security officers, compliance managers

Purpose: Ensure data protection aligns with POPIA, ISO/IEC 27031, and Eskom policies

Topics:

- Data encryption and access control
- Audit logging and reporting
- Data sovereignty and retention compliance
- Risk mitigation (e.g., ransomware recovery)

11. Professional Services for BaaS – Non-Committal

Below is a list of Professional Services typically associated with a Backup as a Service (BaaS) engagement, tailored for an enterprise environment like Eskom and applicable as and when required:

11.1. Assessment and Planning

- Backup environment assessment (current state analysis)
- Data classification and workload prioritisation
- Network and storage capacity planning
- Compliance and regulatory readiness review (e.g., POPIA, ISO/IEC 27031)

11.2. Solution Design

- Architecture design for hybrid/cloud/on-prem backup
- Backup policy and retention strategy development

- Integration planning (e.g., with CMDB, ITOM, RDBMS)
- Security and encryption framework design
- High availability and disaster recovery planning

11.3.Implementation and Configuration

- Deployment of backup agents and infrastructure (disk, tape, cloud)
- Configuration of backup schedules, policies, and replication
- Setup of monitoring, alerting, and reporting tools
- Integration with identity and access management (IAM)
- Network optimisation for backup traffic

11.4.Data Migration and Seeding

- Initial data seeding to backup repositories
- Migration of legacy backup data (if applicable)
- Validation of data integrity post-migration

11.5.Testing and Validation

- Backup and restore testing (including DR scenarios)
- Performance benchmarking
- SLA validation and reporting setup
- Security and access control testing

11.6.Training and Knowledge Transfer

This professional service supports the delivery, handover and enablement of the training requirements defined in Section 10.

- End-user training (self-service restore, folder usage)
- IT support and backup admin training
- DR team and compliance team enablement
- Documentation handover, including backup architecture and data flows.

11.7.Ongoing Support and Optimisation

- Managed services for backup operations
- Periodic health checks and performance tuning

- SLA monitoring and reporting
- Policy reviews and updates
- Incident response and forensic recovery support

11.8. Compliance and Audit Support

- Audit trail configuration and reporting
- Retention policy enforcement
- Support for regulatory audits and internal reviews

12. Professional Services Roles for BaaS

Key roles typically involved in delivering Professional Services for BaaS, tailored for Eskom's enterprise environment, include the following:

12.1. Backup Solutions Architect

- Designs the overall BaaS architecture (on-prem, cloud, hybrid)
- Aligns solution with Eskom's business continuity, compliance, and scalability needs
- Defines backup policies, retention strategies, and integration points

12.2. Backup Implementation Engineer

- Installs and configures backup software and infrastructure
- Deploys agents across servers and endpoints
- Sets up replication, encryption, and monitoring tools

12.3. Data Migration Specialist

- Manages initial data seeding and migration from legacy systems
- Ensures data integrity and consistency during transition
- Coordinates with storage and network teams for performance optimisation

12.4. Disaster Recovery Consultant

- Develops and tests DR scenarios using backup data
- Validates RTO/RPO targets and restore capabilities
- Coordinates with Eskom's DR and IaaS teams

12.5. Security and Compliance Analyst

- Ensures backup processes align with POPIA, ISO/IEC 27031, and Eskom policies
- Configures encryption, access controls, and audit logging
- Supports internal and external audits

12.6. Monitoring and Reporting Specialist

- Implements dashboards and reporting tools
- Tracks SLA metrics (e.g., backup success, restore rates)
- Integrates with CMDB and ITOM platforms

12.7. Training and Enablement Lead

- Develops training materials and conducts workshops
- Supports end-user, EUC, and admin training
- Ensures knowledge transfer and documentation handover

12.8. Project Manager

- Oversees the BaaS implementation lifecycle
- Manages timelines, resources, and stakeholder communication
- Ensures deliverables meet Eskom's expectations

12.9. Support and Optimisation Engineer

- Provides ongoing technical support and issue resolution
- Conducts periodic health checks and performance tuning
- Recommends improvements and updates

13. Responsibility Matrix (RACI)

The responsibility matrix below identifies the indicative RACI allocation for key BaaS professional services activities. Final responsibilities will be confirmed during SLA discussions.

Roles / Activities	Assessment & Planning	Solution Design	Implementat ion &	Data Migration & Seeding	& Testing Validation	Trainin g & Knowl edge Transf er	Ongoing Support & Optimisation	Complian ce & Audit Support
Backup Solutions Architect	R	A	C	C	C	I	I	I
Backup Implementation Engineer	A	R	R	C	C	I	I	I
Data Migration Specialist	C	C	I	R	C	I	I	I
Disaster Recovery Consultant	C	C	I	I	R	I	I	I
Security & Compliance Analyst	C	C	I	I	C	I	I	R
Monitoring & Reporting Specialist	I	I	I	I	I	I	I	I
Training & Enablement Lead	I	I	I	I	I	R	I	I
Project Manager	A	A	A	A	A	A	A	A
Support & Optimisation Engineer	I	I	C	I	I	I	R	I