Annexure D - Work package specifications

For

Specifications for the Work packages related to the supply, installation, commissioning, support, maintenance, monitoring, decommissioning and disposal of Data Protection (Backup and Replication) and Data Storage (Storage Array and Storage Networking) Services for a period of 60 months at Airports Company South Africa

CONTENTS

General Notes

Please take special note of the following items that apply to all Work packages.

- **OEM Warranty –**
    - All hardware must be supplied with a 5-year OEM warranty and software with at least next business day replacement; this includes any firmware or software for the device to function. Some Work packages have other requirements and should be catered for accordingly.

- **Interoperability –**
    - Any OEM can be used to fulfil any work package as long as FULL interoperability is guaranteed within the existing environment.
    - Efforts are made to describe the current environment for all work packages. Please read this information carefully.
    - The bidder can also include the replacement of the up and downstream devices should they wish/need to provide the guarantee.

- **Management –**
    - All supplied devices must be fully managed.
    - Please refer to the currently deployed management software components as per Annexture A – Section 2: Service environment to determine if the proposed hardware will be able to be managed by the in-place management system
    - Should it be needed, the additional management platform must be costed as part of the work package or added to the “Other cost” tab in Annexture C (pricing file)

- **Monitoring –**
    - All supplied devices must be fully monitored.
    - Please refer to the currently deployed monitoring software components as per Annexure A – Section 2: Service environment to determine if the proposed hardware will be able to be monitored by the in-place monitoring system
    - Should it be needed, the additional monitoring platform must be costed as part of the work package or added to the “Other cost” tab in Annexure C (pricing file)

- **Support –**
    - Any proposed OEMs must be fully supported by the bidder using OEM certified staff at the equivalent requested certification levels.

1.0 Work Package: Backup Solution - Replacement - Specification A

1.1 Short Description

Supply, physically install and configure devices that meet enterprise-grade backup hardware and software specifications or the latest equivalent standards to replace existing devices that have reached the end of life.

1.2 As-is environment:

Backups are performed at the major airports: OR Tambo (JNB), Cape Town (CPT), King Shaka (DUR), using Dell Avamar backup servers with separate scalable backup storage systems (Dell Data Domain) as target devices. Backups are performed on the local area network at each airport, moving information off the primary source (the servers) to separate hardware. Critical data is then replicated offsite to a secondary or offsite location for safekeeping.

1.3 To/be Requirement:

The specification devices must have the following features:

- The solution should have a minimum of 600 TB usable storage (or to the closest 1 TB).
- All associated licenses should be included for a minimum of five (5) years (centralised management console, reporting, capacity, replication, data-hold, retention, encryption, client and all other feature licenses).
- All firmware and software version upgrades should be included for a minimum of five (5) years.
- All Hardware must be covered with 5-year warranty with a 6-hour fix.
- Vendor support is mandatory to maintain operational continuity and compliance with data protection regulations.
- Must be able to scale to accommodate future data growth.
- May incorporate a combination of backup appliances and backup storage devices to deliver a unified, consolidated backup solution.
- Supports full, incremental, differential, and continuous data protection (CDP) backups with automated, policy-based scheduling.
- Removes duplicate data blocks and compresses backups to optimise storage efficiency.
- Handles data at scale; protects Virtual machines (VMware, Hyper-V, etc.), physical servers, cloud (AWS, Azure), Kubernetes, databases (SQL, Oracle, etc), Microsoft SharePoint and email Microsoft Exchange.
- Support for various backups, including on-premises, cloud-native, or hybrid functionality with direct-to-cloud backups, tiering, and replication.
- Instant recovery, granular restore (files/folders/emails), bare-metal restore, and VM instant boot.
- Site recovery orchestration, failover/failback, automated DR testing, and replication to secondary sites/cloud.
- Encryption (at rest/in-flight, AES-256), immutability/air-gapping, malware scanning, anomaly detection, and role-based access control (RBAC/MFA).
- Single-pane console for monitoring, reporting, analytics, and policy enforcement across all environments.
- Long-term retention policies, audit logs, and support for regulations (GDPR, HIPAA, etc.).
- Policy-driven automation, AI-based insights for anomalies, predictive analytics, and self-healing features.

- Be able to integrate with existing backup software to allow for restoring existing backups. If separate hardware is required for this, add this to the solution.
- Support high-speed data transfer rates to minimise backup windows.
- The solution must include redundancy features, such as RAID configurations, dual power supplies, dual controllers, and multiple connectivity modules.
- Support for immutable backups to protect against ransomware.
- The hardware must be deployed with minimal downtime, requiring a phased implementation plan and comprehensive testing to ensure reliability.
- Any proposed OEMs must be fully supported by the bidder using OEM-certified staff at the equivalent requested certification levels.

1.4 Work Package Special Notes / Terms:

- Provide Documentation (as built and update of existing documents/drawings)
- Asset tag of hardware
- Follow the ACSA capitalisation process
- Labelling as per ACSA standards
- Include project management services
- Work will be performed after hours and must be costed accordingly
- Physical installation, configuration and commissioning of work package equipment
- Decommissioning, un-racking, packaging and moving to the storeroom of replaced equipment

2.0 Work Package: Backup Solution - Replacement - Specification B

2.1 Short Description

Supply, physically install and configure devices that meet enterprise-grade backup hardware and software specifications or the latest equivalent standards to replace existing devices that have reached end of life.

2.2 As-is environment:

Backups are performed at the major airports: OR Tambo (JNB), Cape Town (CPT), King Shaka (DUR), using Dell Avamar backup servers with separate scalable backup storage systems (Dell Data Domain) as target devices. Backups are performed on the local area network at each airport, moving information off the primary source (the servers) to separate hardware. Critical data is then replicated offsite to a secondary or offsite location for safekeeping.

2.3 To/be Requirement:

The specification devices must have the following features:

- The solution should have a minimum of 200 TB usable storage (or to the closest 1 TB)
- All associated licenses should be included for a minimum of five (5) years (centralised management console, reporting, capacity, replication, data-hold, retention, encryption, client and all other feature licenses).
- All firmware and software version upgrades should be included for a minimum of five (5) years.
- All Hardware must be covered with 5-year warranty with a 6-hour fix.
- Vendor support is mandatory to maintain operational continuity and compliance with data protection regulations.
- Must be able to scale to accommodate future data growth.
- May incorporate a combination of backup appliances and backup storage devices to deliver a unified, consolidated backup solution.
- Supports full, incremental, differential, and continuous data protection (CDP) backups with automated, policy-based scheduling.
- Removes duplicate data blocks and compresses backups to optimise storage efficiency.
- Handles data at scale; protects Virtual machines (VMware, Hyper-V, etc.), physical servers, cloud (AWS, Azure), Kubernetes, databases (SQL, Oracle, etc), Microsoft SharePoint and email Microsoft Exchange.
- Support for various backups, including on-premises, cloud-native, or hybrid functionality with direct-to-cloud backups, tiering, and replication.
- Instant recovery, granular restore (files/folders/emails), bare-metal restore, and VM instant boot.
- Site recovery orchestration, failover/failback, automated DR testing, and replication to secondary sites/cloud.
- Encryption (at rest/in-flight, AES-256), immutability/air-gapping, malware scanning, anomaly detection, and role-based access control (RBAC/MFA).
- Single-pane console for monitoring, reporting, analytics, and policy enforcement across all environments.
- Long-term retention policies, audit logs, and support for regulations (GDPR, HIPAA, etc.).
- Policy-driven automation, AI-based insights for anomalies, predictive analytics, and self-healing features.

- Be able to integrate with existing backup software to allow for restoring existing backups. If separate hardware is required for this, add this to the solution.
- Support high-speed data transfer rates to minimise backup windows.
- The solution must include redundancy features, such as RAID configurations, dual power supplies, dual controllers, and multiple connectivity modules.
- Support for immutable backups to protect against ransomware.
- The hardware must be deployed with minimal downtime, requiring a phased implementation plan and comprehensive testing to ensure reliability.
- Any proposed OEMs must be fully supported by the bidder using OEM-certified staff at the equivalent requested certification levels.

2.4 Work Package Special Notes / Terms:

- Provide Documentation (as built and update of existing documents/drawings)
- Asset tag of hardware
- Follow the ACSA capitalisation process
- Labelling as per ACSA standards
- Include project management services
- Work will be performed after hours and must be costed accordingly
- Physical installation, configuration and commissioning of work package equipment
- Decommissioning, un-racking, packaging and moving to the storeroom of replaced equipment

3.0 Work Package: Backup Solution - Replacement - Specification C

3.1 Short Description

Supply, physically install and configure devices that meet enterprise-grade backup hardware and software specifications or the latest equivalent standards to replace existing devices that have reached end of life.

3.2 As-is environment:

Backups are performed at the major airports: OR Tambo (JNB), Cape Town (CPT), King Shaka (DUR), using Dell Avamar backup servers with separate scalable backup storage systems (Dell Data Domain) as target devices. Backups are performed on the local area network at each airport, moving information off the primary source (the servers) to separate hardware. Critical data is then replicated offsite to a secondary or offsite location for safekeeping.

3.3 To/be Requirement:

The specification devices must have the following features:

- The solution should have a minimum of 100 TB usable storage (or to the closest 1 TB)
- All associated licenses should be included for a minimum of five (5) years (centralised management console, reporting, capacity, replication, data-hold, retention, encryption, client and all other feature licenses).
- All firmware and software version upgrades should be included for a minimum of five (5) years.
- All Hardware must be covered with 5-year warranty with a 6-hour fix.
- Vendor support is mandatory to maintain operational continuity and compliance with data protection regulations.
- Must be able to scale to accommodate future data growth.
- May incorporate a combination of backup appliances and backup storage devices to deliver a unified, consolidated backup solution.
- Supports full, incremental, differential, and continuous data protection (CDP) backups with automated, policy-based scheduling.
- Removes duplicate data blocks and compresses backups to optimise storage efficiency.
- Handles data at scale; protects Virtual machines (VMware, Hyper-V, etc.), physical servers, cloud (AWS, Azure), Kubernetes, databases (SQL, Oracle, etc), Microsoft SharePoint and email Microsoft Exchange.
- Support for various backups, including on-premises, cloud-native, or hybrid functionality with direct-to-cloud backups, tiering, and replication.
- Instant recovery, granular restore (files/folders/emails), bare-metal restore, and VM instant boot.
- Site recovery orchestration, failover/failback, automated DR testing, and replication to secondary sites/cloud.
- Encryption (at rest/in-flight, AES-256), immutability/air-gapping, malware scanning, anomaly detection, and role-based access control (RBAC/MFA).
- Single-pane console for monitoring, reporting, analytics, and policy enforcement across all environments.
- Long-term retention policies, audit logs, and support for regulations (GDPR, HIPAA, etc.).
- Policy-driven automation, AI-based insights for anomalies, predictive analytics, and self-healing features.

- Be able to integrate with existing backup software to allow for restoring existing backups. If separate hardware is required for this, add this to the solution.
- Support high-speed data transfer rates to minimise backup windows.
- The solution must include redundancy features, such as RAID configurations, dual power supplies, dual controllers, and multiple connectivity modules.
- Support for immutable backups to protect against ransomware.
- The hardware must be deployed with minimal downtime, requiring a phased implementation plan and comprehensive testing to ensure reliability.
- Any proposed OEMs must be fully supported by the bidder using OEM-certified staff at the equivalent requested certification levels.

3.4 **Work Package Special Notes / Terms:**

- Provide Documentation (as built and update of existing documents/drawings)
- Asset tag of hardware
- Follow the ACSA capitalisation process
- Labelling as per ACSA standards
- Include project management services
- Work will be performed after hours and must be costed accordingly
- Physical installation, configuration and commissioning of work package equipment
- Decommissioning, un-racking, packaging and moving to the storeroom of replaced equipment

4.0 Work Package: Backup Solution - Replacement - Specification D

4.1 Short Description

Supply, physically install and configure devices that meet enterprise-grade backup hardware and software specifications or latest equivalent standards to replace existing devices that have reached end of life.

4.2 As-is environment:

Backups are performed at the regional airports: Chief Dawid Stuurman (PLZ), Bram Fischer (BFN), King Phalo (ELS), George (GRJ), Upington (UTN) and Kimberly (KIM) airports using Dell Avamar backup appliances consisting of a backup server with internal storage. Backups are performed on the local area network at each airport, moving information off the primary source (the servers) to separate hardware. Critical data is then replicated offsite to a secondary or offsite location for safe keeping.

4.3 To/be Requirement:

The specification devices must have the following features:

- The solution should have a minimum of 20 TB usable storage (or to the closest 1 TB)
- All associated licenses should be included for a minimum of five (5) years (centralised management console, reporting, capacity, replication, data-hold, retention, encryption, client and all other feature licenses).
- All firmware and software version upgrades should be included for a minimum of five (5) years.
- All Hardware must be covered with 5-year warranty with a 6-hour fix.
- Vendor support is mandatory to maintain operational continuity and compliance with data protection regulations.
- Must be able to scale to accommodate future data growth.
- May incorporate a combination of backup appliances and backup storage devices to deliver a unified, consolidated backup solution.
- Supports full, incremental, differential, and continuous data protection (CDP) backups with automated, policy-based scheduling.
- Removes duplicate data blocks and compresses backups to optimise storage efficiency.
- Handles data at scale; protects Virtual machines (VMware, Hyper-V, etc.), physical servers, cloud (AWS, Azure), Kubernetes, databases (SQL, Oracle, etc), Microsoft SharePoint and email Microsoft Exchange.
- Support for various backups, including on-premises, cloud-native, or hybrid functionality with direct-to-cloud backups, tiering, and replication.
- Instant recovery, granular restore (files/folders/emails), bare-metal restore, and VM instant boot.
- Site recovery orchestration, failover/failback, automated DR testing, and replication to secondary sites/cloud.
- Encryption (at rest/in-flight, AES-256), immutability/air-gapping, malware scanning, anomaly detection, and role-based access control (RBAC/MFA).
- Single-pane console for monitoring, reporting, analytics, and policy enforcement across all environments.
- Long-term retention policies, audit logs, and support for regulations (GDPR, HIPAA, etc.).
- Policy-driven automation, AI-based insights for anomalies, predictive analytics, and self-healing features.

- Be able to integrate with existing backup software to allow for restoring existing backups. If separate hardware is required for this, add this to the solution.
- Support high-speed data transfer rates to minimise backup windows.
- The solution must include redundancy features, such as RAID configurations, dual power supplies, dual controllers, and multiple connectivity modules.
- Support for immutable backups to protect against ransomware.
- The hardware must be deployed with minimal downtime, requiring a phased implementation plan and comprehensive testing to ensure reliability.
- Any proposed OEMs must be fully supported by the bidder using OEM-certified staff at the equivalent requested certification levels.

4.4 Work Package Special Notes / Terms:

- Provide Documentation (as built and update of existing documents/drawings)
- Asset tag of hardware
- Follow the ACSA capitalisation process
- Labelling as per ACSA standards
- Include project management services
- Work will be performed after hours and must be costed accordingly
- Physical installation, configuration and commissioning of work package equipment
- Decommissioning, un-racking, packaging and moving to the storeroom of replaced equipment

5.0 Work Package: Backup Solution - Replacement - Specification E

5.1 Short Description

Supply, physically install and configure devices that meet enterprise-grade backup hardware and software specifications or latest equivalent standards to replace existing devices that have reached end of life.

5.2 As-is environment:

Backups are performed at the regional airports: Chief Dawid Stuurman (PLZ), Bram Fischer (BFN), King Phalo (ELS), George (GRJ), Upington (UTN) and Kimberly (KIM) airports using Dell Avamar backup appliances consisting of a backup server with internal storage. Backups are performed on the local area network at each airport, moving information off the primary source (the servers) to separate hardware. Critical data is then replicated offsite to a secondary or offsite location for safe keeping.

5.3 To/be Requirement:

The specification devices must have the following features:

- The solution should have a minimum of 10 TB usable storage (or to the closest 1 TB)
- All associated licenses should be included for a minimum of five (5) years (centralised management console, reporting, capacity, replication, data-hold, retention, encryption, client and all other feature licenses).
- All firmware and software version upgrades should be included for a minimum of five (5) years.
- All Hardware must be covered with 5-year warranty with a 6-hour fix.
- Vendor support is mandatory to maintain operational continuity and compliance with data protection regulations.
- Must be able to scale to accommodate future data growth.
- May incorporate a combination of backup appliances and backup storage devices to deliver a unified, consolidated backup solution.
- Supports full, incremental, differential, and continuous data protection (CDP) backups with automated, policy-based scheduling.
- Removes duplicate data blocks and compresses backups to optimise storage efficiency.
- Handles data at scale; protects Virtual machines (VMware, Hyper-V, etc.), physical servers, cloud (AWS, Azure), Kubernetes, databases (SQL, Oracle, etc), Microsoft SharePoint and email Microsoft Exchange.
- Support for various backups, including on-premises, cloud-native, or hybrid functionality with direct-to-cloud backups, tiering, and replication.
- Instant recovery, granular restore (files/folders/emails), bare-metal restore, and VM instant boot.
- Site recovery orchestration, failover/failback, automated DR testing, and replication to secondary sites/cloud.
- Encryption (at rest/in-flight, AES-256), immutability/air-gapping, malware scanning, anomaly detection, and role-based access control (RBAC/MFA).
- Single-pane console for monitoring, reporting, analytics, and policy enforcement across all environments.
- Long-term retention policies, audit logs, and support for regulations (GDPR, HIPAA, etc.).
- Policy-driven automation, AI-based insights for anomalies, predictive analytics, and self-healing features.

- Be able to integrate with existing backup software to allow for restoring existing backups. If separate hardware is required for this, add this to the solution.
- Support high-speed data transfer rates to minimise backup windows.
- The solution must include redundancy features, such as RAID configurations, dual power supplies, dual controllers, and multiple connectivity modules.
- Support for immutable backups to protect against ransomware.
- The hardware must be deployed with minimal downtime, requiring a phased implementation plan and comprehensive testing to ensure reliability.
- Any proposed OEMs must be fully supported by the bidder using OEM-certified staff at the equivalent requested certification levels.

5.4 Work Package Special Notes / Terms:

- Provide Documentation (as built and update of existing documents / drawings)
- Asset tag of hardware
- Follow ACSA capitalisation process
- Labelling as per ACSA standards
- Include project management services
- Work will be performed after hours and must be costed accordingly
- Physical installation, configuration and commissioning of work package equipment
- Decommissioning, un-racking, packaging and moving to storeroom of replaced equipment

6.0 Work Package: Backup Solution - Capacity Upgrade - Specification A

6.1 Short Description

Supply, physically install and configure additional storage capacity, including expansion shelves and various enterprise drives to expand existing backup devices.

6.2 As-is environment:

Backups storage systems are currently deployed at the major airports: OR Tambo (JNB), Cape Town (CPT), King Shaka (DUR). These sites are utilising different models according to the capacity and performance requirements. Dell PowerProtect DP5900 devices are installed at OR Tambo and Cape Town with additional Dell PowerProtect DD9410 backup storage device. For King Shaka, Dell PowerProtect DP4400 devices are installed with an additional Dell PowerProtect DD6410 backup storage device soon to be added. Backups are performed on the local area network at each airport, moving information off the primary source (the servers) to separate hardware. Critical data is then replicated offsite to a secondary or offsite location for safe keeping.

6.3 To/be Requirement:

The specification devices must have the following features:

- The expansion solution should have a minimum of 100 TB usable storage (or to the closest 1 TB) and should include all required hardware needed to achieve this. This includes expansions shelves, cabling, sfps, etc.
- All associated licenses should be included for a minimum five (5) years (centralised management console, reporting, capacity, replication, data-hold, retention, encryption, client and all other feature licenses).
- All firmware and software version upgrades should be included for a minimum five (5) years.
- All Hardware must be covered with 5-year warranty with a 6-hour fix.
- Vendor support is mandatory to maintain operational continuity and compliance with data protection regulations.
- The solution must include redundancy features, such as RAID configurations, dual power supplies, dual controllers, multiple connectivity modules.
- The hardware must be deployed with minimal downtime, requiring a phased implementation plan and comprehensive testing to ensure reliability.
- Any proposed OEMs must be fully supported by the bidder using OEM-certified staff at the equivalent requested certification levels.

6.4 Work Package Special Notes / Terms:

- Provide Documentation (as built and update of existing documents / drawings)
- Asset tag of hardware
- Follow ACSA capitalisation process
- Labelling as per ACSA standards
- Include project management services
- Work will be performed after hours and must be costed accordingly
- Physical installation, configuration and commissioning of work package equipment
- Decommissioning, un-racking, packaging and moving to storeroom of replaced equipment

7.0 Work Package: Backup Solution - Capacity Upgrade - Specification B

7.1 Short Description

Supply, physically install and configure additional storage capacity, including expansion shelves and various enterprise drives to expand existing backup devices.

7.2 As-is environment:

Backups storage systems are currently deployed at the major airports: OR Tambo (JNB), Cape Town (CPT), King Shaka (DUR). These sites are utilising different models according to the capacity and performance requirements. Dell PowerProtect DP5900 devices are installed at OR Tambo and Cape Town with additional Dell PowerProtect DD9410 backup storage device. For King Shaka, Dell PowerProtect DP4400 devices are installed with an additional Dell PowerProtect DD6410 backup storage device soon to be added. Backups are performed on the local area network at each airport, moving information off the primary source (the servers) to separate hardware. Critical data is then replicated offsite to a secondary or offsite location for safe keeping.

7.3 To/be Requirement:

The specification devices must have the following features:

- The expansion solution should have a minimum of 10 TB usable storage (or to the closest 1 TB) and should include all required hardware needed to achieve this. This includes expansions shelves, cabling, sfps, etc.
- All associated licenses should be included for a minimum five (5) years (centralised management console, reporting, capacity, replication, data-hold, retention, encryption, client and all other feature licenses).
- All firmware and software version upgrades should be included for a minimum five (5) years.
- All Hardware must be covered with 5-year warranty with a 6-hour fix.
- Vendor support is mandatory to maintain operational continuity and compliance with data protection regulations.
- The solution must include redundancy features, such as RAID configurations, dual power supplies, dual controllers, multiple connectivity modules.
- The hardware must be deployed with minimal downtime, requiring a phased implementation plan and comprehensive testing to ensure reliability.
- Any proposed OEMs must be fully supported by the bidder using OEM-certified staff at the equivalent requested certification levels.

7.4 Work Package Special Notes / Terms:

- Provide Documentation (as built and update of existing documents / drawings)
- Asset tag of hardware
- Follow ACSA capitalisation process
- Labelling as per ACSA standards
- Include project management services
- Work will be performed after hours and must be costed accordingly
- Physical installation, configuration and commissioning of work package equipment
- Decommissioning, un-racking, packaging and moving to storeroom of replaced equipment

8.0 Work Package: Backup Solution - Capacity Upgrade - Specification C

8.1 Short Description

Supply, physically install and configure additional storage capacity, including expansion shelves and various enterprise drives to expand existing backup devices.

8.2 As-is environment:

Backups storage systems are currently deployed at the major airports: OR Tambo (JNB), Cape Town (CPT), King Shaka (DUR). These sites are utilising different models according to the capacity and performance requirements. Dell PowerProtect DP5900 devices are installed at OR Tambo and Cape Town with additional Dell PowerProtect DD9410 backup storage device. For King Shaka, Dell PowerProtect DP4400 devices are installed with an additional Dell PowerProtect DD6410 backup storage device soon to be added. Backups are performed on the local area network at each airport, moving information off the primary source (the servers) to separate hardware. Critical data is then replicated offsite to a secondary or offsite location for safe keeping.

8.3 To/be Requirement:

The specification devices must have the following features:

- The expansion solution should have a minimum of 1 TB usable storage (or to the closest 1 TB) and should include all required hardware needed to achive this. This includes expansions shelves, cabling, sfps, etc.
- All associated licenses should be included for a minimum five (5) years (centralised management console, reporting, capacity, replication, data-hold, retention, encryption, client and all other feature licenses).
- All firmware and software version upgrades should be included for a minimum five (5) years.
- All Hardware must be covered with 5-year warranty with a 6-hour fix.
- Vendor support is mandatory to maintain operational continuity and compliance with data protection regulations.
- The solution must include redundancy features, such as RAID configurations, dual power supplies, dual controllers, multiple connectivity modules.
- The hardware must be deployed with minimal downtime, requiring a phased implementation plan and comprehensive testing to ensure reliability.
- Any proposed OEMs must be fully supported by the bidder using OEM-certified staff at the equivalent requested certification levels.

8.4 Work Package Special Notes / Terms:

- Provide Documentation (as built and update of existing documents / drawings)
- Asset tag of hardware
- Follow ACSA capitalisation process
- Labelling as per ACSA standards
- Include project management services
- Work will be performed after hours and must be costed accordingly
- Physical installation, configuration and commissioning of work package equipment
- Decommissioning, un-racking, packaging and moving to storeroom of replaced equipment

9.0 Work Package: CCTV Storage Solution - Replacement - Specification A

9.1 Short Description

Supply, physically install and configure replacement storage devices that are certified for CCTV use. It should be certified and support the FLIR CCTV system.

9.2 As-is environment:

Security systems consist of cameras, cabling infrastructure, servers and dedicated storage. These systems are deployed at all sites. Currently there are multiple CCTV storage systems deployed across all airports in various configuration and sizes.

The following design is followed at all major airports: OR Tambo (JNB), Cape Town (CPT), King Shaka (DUR): Multiple virtual servers (Archivers) servers are presented with storage from 2 dedicated CCTV storage systems via a SAN fabric network. The capacity of each array is split and allocated to each server, allowing storage form both storage devices to be allocated to each VM, providing redundancy.

9.3 To/be Requirement:

Replace the distributed CCTV storage arrays with two (2) centralised shared storage arrays per site, split over 2 rooms and connected via redundant fibre channel fabrics. The two (2) shared storage systems will provide redundancy as well as consolidate all storage into less devices to manage and maintain, only growing the storage capacity as needed. Connectivity between storage and server devices should be done via FC SAN switches via two (2) dedicated redundant fabrics. Storage arrays and SAN switches should be CCTV system compatible with fabric version GEN 7 or higher support.
The specification devices must have the following features:

- The solution must include redundancy features, such as RAID configurations, dual power supplies, dual controllers, multiple connectivity modules, Redundant dual-sockets.
- Support for Flash (SSD), SAS, NL-SAS drives
- Drive Enclosures supported with the ability to expand with additional enclosures up to 10 PB
- Inline deduplication + compression
- Caching options for tiering
- Supported RAID Configurations: 1/0, 5, 6
- Backend Connectivity: 12 Gb/s SAS (multiple lane options)
- Protocols: Block (FC, iSCSI), File (NFS/SMB), vVols
- Replication, snapshots, thin provisioning, QoS
- All associated licenses should be included for a minimum five (5) years (centralised management console, reporting, capacity, replication, data-hold, retention, encryption, client and all other feature licenses).
- All firmware and software version upgrades should be included for a minimum five (5) years.
- All Hardware must be covered with 5-year warranty with a 6-hour fix.
- Vendor support is mandatory to maintain operational continuity and compliance with data protection regulations.
- Must be able to scale to accommodate future data growth.
- Data Encryption (AES-256) support, with KMIP support
- Single-pane console for monitoring, reporting, analytics, and policy enforcement across all environments.
- Support for immutable backups to protect against ransomware.

- The hardware must be deployed with minimal downtime, requiring a phased implementation plan and comprehensive testing to ensure reliability.
- Any proposed OEMs must be fully supported by the bidder using OEM-certified staff at the equivalent requested certification levels.

9.4 Work Package Special Notes / Terms:

- Provide Documentation (as built and update of existing documents / drawings)
- Asset tag of hardware
- Follow ACSA capitalisation process
- Labelling as per ACSA standards
- Include project management services
- Work will be performed after hours and must be costed accordingly
- Physical installation, configuration and commissioning of work package equipment
- Decommissioning, un-racking, packaging and moving to storeroom of replaced equipment

10.0 Work Package: CCTV Storage Solution - Replacement - Specification B

10.1 Short Description

Supply, physically install and configure replacement storage devices that are certified for CCTV use. It should be certified and support the FLIR CCTV system.

10.2 As-is environment:

Security systems consist of cameras, cabling infrastructure, servers and dedicated storage. These systems are deployed at all sites. Currently there are multiple CCTV storage systems deployed across all airports in various configuration and sizes.

The following design is followed at all major airports: OR Tambo (JNB), Cape Town (CPT), King Shaka (DUR): Multiple virtual servers (Archivers) servers are presented with storage from 2 dedicated CCTV storage systems via a SAN fabric network. The capacity of each array is split and allocated to each server, allowing storage form both storage devices to be allocated to each VM, providing redundancy.

10.3 To/be Requirement:

Replace the distributed CCTV storage arrays with two (2) centralised shared storage arrays per site, split over 2 rooms and connected via redundant fiber channel fabrics. The two (2) shared storage systems will provide redundancy as well as consolidate all storage into less devices to manage and maintain, only growing the storage capacity as needed. Connectivity between storage and server devices should be done via FC SAN switches via two (2) dedicated redundant fabrics. Storage arrays and SAN switches should be CCTV system compatible with fabric version GEN 7 or higher support.
The specification devices must have the following features:

- The solution must include redundancy features, such as RAID configurations, dual power supplies, dual controllers, multiple connectivity modules, Redundant dual-sockets.
- Support for Flash (SSD), SAS, NL-SAS drives
- Drive Enclosures supported with the ability to expand with additional enclosures up to 6 PB
- Inline deduplication + compression
- Caching options for tiering
- Supported RAID Configurations: 1/0, 5, 6
- Backend Connectivity: 12 Gb/s SAS (multiple lane options)
- Protocols: Block (FC, iSCSI), File (NFS/SMB), vVols
- Replication, snapshots, thin provisioning, QoS
- All associated licenses should be included for a minimum five (5) years (centralised management console, reporting, capacity, replication, data-hold, retention, encryption, client and all other feature licenses).
- All firmware and software version upgrades should be included for a minimum five (5) years.
- All Hardware must be covered with 5-year warranty with a 6-hour fix.
- Vendor support is mandatory to maintain operational continuity and compliance with data protection regulations.
- Must be able to scale to accommodate future data growth.
- Data Encryption (AES-256) support, with KMIP support
- Single-pane console for monitoring, reporting, analytics, and policy enforcement across all environments.
- Support for immutable backups to protect against ransomware.

- The hardware must be deployed with minimal downtime, requiring a phased implementation plan and comprehensive testing to ensure reliability.
- Any proposed OEMs must be fully supported by the bidder using OEM-certified staff at the equivalent requested certification levels.

10.4 Work Package Special Notes / Terms:

- Provide Documentation (as built and update of existing documents / drawings)
- Asset tag of hardware
- Follow ACSA capitalisation process
- Labelling as per ACSA standards
- Include project management services
- Work will be performed after hours and must be costed accordingly
- Physical installation, configuration and commissioning of work package equipment
- Decommissioning, un-racking, packaging and moving to storeroom of replaced equipment

11.0 Work Package: CCTV Storage Solution - Replacement - Specification C

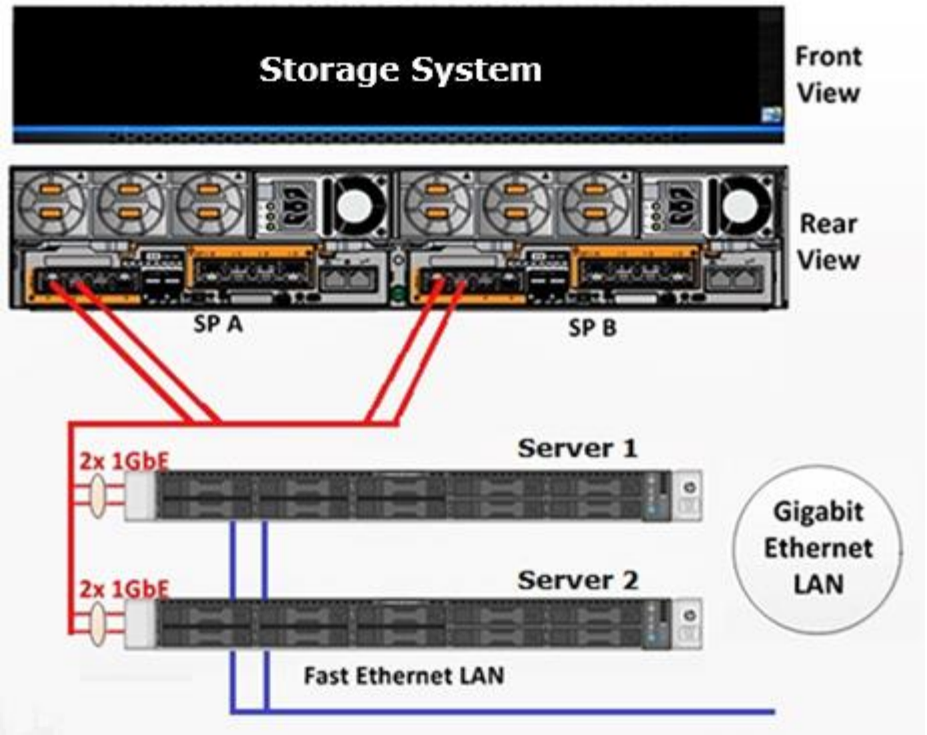
11.1 Short Description

Supply, physically install and configure replacement storage devices that are certified for CCTV use. It should be certified and support the FLIR CCTV system.

11.2 As-is environment:

Security systems consist of cameras, cabling infrastructure, servers and dedicated storage. These systems are deployed at all sites. Currently there are multiple CCTV storage systems deployed across all airports in various configuration and sizes.

The following design is followed at all regional airports: Chief Dawid Stuurman (PLZ), Bram Fischer (BFN), King Phalo (ELS), George (GRJ), Upington (UTN) and Kimberly (KIM): Two (2) servers are directly connected via multi-mode fiber to a separate storage system. The capacity of each array is split and allocated to each server, allowing storage form both storage devices to be allocated to each physical server, providing redundancy.



The solution consists of the following:

Site	Current Number of storage systems per site (each with two hosts)
Chief Dawid Stuurman International Airport - Gqeberha (PLZ)	2
Bram Fischer International Airport - Bloemfontein (BFN)	1
King Phalo Airport - East London (ELS)	2
George Airport - George (GRJ)	2
Kimberley Airport - Kimberley (KIM)	2
Upington International Airport - Upington (UTN)	1

11.3 To/be Requirement:

Replace the distributed CCTV storage arrays with one (1) centralised shared storage arrays per site and connected via a redundant fiber channel fabric. The shared storage system will provide redundancy as well as consolidate all storage into less devices to manage and maintain, only growing the storage capacity centrally as needed. Connectivity between storage and server devices should be done via FC SAN switches creating a dedicated redundant fabric. Storage arrays and SAN switches should be CCTV system compatible with fabric version GEN 7 or higher support.

The specification devices must have the following features:

- The solution must include redundancy features, such as RAID configurations, dual power supplies, dual controllers, multiple connectivity modules, Redundant dual-sockets.
- Support for Flash (SSD), SAS, NL-SAS drives
- Drive Enclosures supported with the ability to expand with additional enclosures up to 1 PB
- Inline deduplication + compression
- Caching options for tiering
- Supported RAID Configurations: 1/0, 5, 6
- Backend Connectivity: 12 Gb/s SAS (multiple lane options)
- Protocols: Block (FC, iSCSI), File (NFS/SMB), vVols
- Replication, snapshots, thin provisioning, QoS
- All associated licenses should be included for a minimum five (5) years (centralised management console, reporting, capacity, replication, data-hold, retention, encryption, client and all other feature licenses).
- All firmware and software version upgrades should be included for a minimum five (5) years.
- All Hardware must be covered with 5-year warranty with a 6-hour fix.
- Vendor support is mandatory to maintain operational continuity and compliance with data protection regulations.
- Must be able to scale to accommodate future data growth.
- Data Encryption (AES-256) support, with KMIP support
- Single-pane console for monitoring, reporting, analytics, and policy enforcement across all environments.
- Support for immutable backups to protect against ransomware.
- The hardware must be deployed with minimal downtime, requiring a phased implementation plan and comprehensive testing to ensure reliability.
- Any proposed OEMs must be fully supported by the bidder using OEM-certified staff at the equivalent requested certification levels.

11.4 Work Package Special Notes / Terms:

- Provide Documentation (as built and update of existing documents / drawings)
- Asset tag of hardware
- Follow ACSA capitalisation process
- Labelling as per ACSA standards
- Include project management services
- Work will be performed after hours and must be costed accordingly
- Physical installation, configuration and commissioning of work package equipment
- Decommissioning, un-racking, packaging and moving to storeroom of replaced equipment

11.5 Work Package Special Notes / Terms:

- Provide Documentation (as built and update of existing documents / drawings)
- Asset tag of hardware
- Follow ACSA capitalisation process
- Labelling as per ACSA standards
- Include project management services
- Work will be performed after hours and must be costed accordingly
- Physical installation, configuration and commissioning of work package equipment
- Decommissioning, un-racking, packaging and moving to storeroom of replaced equipment

12.0 Work Package: Shared Storage Solution - Replacement - Specification A

12.1 Short Description

Supply, physically install and configure replacement storage devices that are used for shared workloads and long term storage.

12.2 As-is environment:

The production and DR shared storage environments, utilize Dell Unity storage arrays to provide LUNS to physical servers (HPE Blade System C7000 BL-series) as block storage as well as VMFS datastores to VMware and Hyper-V. The existing shared storage systems currently do not cater for any tiering or archiving functionality. These are flash only devices hosting all the current data. It is connected to 2 x identical 16Gbps local fiber fabrics (Dell Connectrix B6620D switches) hosted at JNB, CPT and DUR. Each of the two data centre rooms per site, has two (2) storage systems to provide for redundancy and failover across the two rooms.

OR Tambo (JNB): 2 x Unity 500F
Cape Town (CPT): 2 x Unity 450F
King Shaka (DUR): 2 x Unity 450F

OR Tambo (JNB) DR: 1 x Unity 450F
Cape Town (CPT) DR: 1 x Unity 450F

12.3 To/be Requirement:

Replace the distributed storage arrays with two (2) centralised shared storage arrays per site, split over 2 rooms and connected via redundant fiber channel fabrics. The two (2) shared storage systems will provide redundancy as well as consolidate all storage into less devices to manage and maintain, only growing the storage capacity as needed. Connectivity between storage and server devices should be done via FC SAN switches via two (2) dedicated redundant fabrics. Storage arrays and SAN switches should be compatible with fabric version GEN 7 or higher support.
The specification devices must have the following features:

- The solution must include redundancy features, such as RAID configurations, dual power supplies, dual controllers, multiple connectivity modules, Redundant dual-sockets.
- Support for Flash (SSD), SAS, NL-SAS drives
- Drive Enclosures supported with the ability to expand with additional enclosures up to 10 PB
- Inline deduplication + compression
- Caching options for tiering
- Supported RAID Configurations: 1/0, 5, 6
- Backend Connectivity: 12 Gb/s SAS (multiple lane options)
- Protocols: Block (FC, iSCSI), File (NFS/SMB), vVols
- Replication, snapshots, thin provisioning, QoS
- All associated licenses should be included for a minimum five (5) years (centralised management console, reporting, capacity, replication, data-hold, retention, encryption, client and all other feature licenses).
- All firmware and software version upgrades should be included for a minimum five (5) years.
- All Hardware must be covered with 5-year warranty with a 6-hour fix.
- Vendor support is mandatory to maintain operational continuity and compliance with data protection regulations.

- Must be able to scale to accommodate future data growth.
- Data Encryption (AES-256) support, with KMIP support
- Single-pane console for monitoring, reporting, analytics, and policy enforcement across all environments.
- Support for immutable backups to protect against ransomware.
- The hardware must be deployed with minimal downtime, requiring a phased implementation plan and comprehensive testing to ensure reliability.
- Any proposed OEMs must be fully supported by the bidder using OEM-certified staff at the equivalent requested certification levels.

12.4 Work Package Special Notes / Terms:

- Provide Documentation (as built and update of existing documents / drawings)
- Asset tag of hardware
- Follow ACSA capitalisation process
- Labelling as per ACSA standards
- Include project management services
- Work will be performed after hours and must be costed accordingly
- Physical installation, configuration and commissioning of work package equipment
- Decommissioning, un-racking, packaging and moving to storeroom of replaced equipment

13.0 Work Package: Shared Storage Solution - Replacement - Specification B

13.1 Short Description

Supply, physically install and configure replacement storage devices that are used for shared workloads and long term storage.

13.2 As-is environment:

The production and DR shared storage environments, utilize Dell Unity storage arrays to provide LUNS to physical servers (HPE Blade System C7000 BL-series) as block storage as well as VMFS datastores to VMware and Hyper-V. The existing shared storage systems currently do not cater for any tiering or archiving functionality. These are flash only devices hosting all the current data. It is connected to 2 x identical 16Gbps local fiber fabrics (Dell Connectrix B6620D switches) hosted at JNB, CPT and DUR. Each of the two data centre rooms per site, has two (2) storage systems to provide for redundancy and failover across the two rooms.

OR Tambo (JNB): 2 x Unity 500F
Cape Town (CPT): 2 x Unity 450F
King Shaka (DUR): 2 x Unity 450F

OR Tambo (JNB) DR: 1 x Unity 450F
Cape Town (CPT) DR: 1 x Unity 450F

13.3 To/be Requirement:

Replace the distributed storage arrays with two (2) centralised shared storage arrays per site, split over 2 rooms and connected via redundant fiber channel fabrics. The two (2) shared storage systems will provide redundancy as well as consolidate all storage into less devices to manage and maintain, only growing the storage capacity as needed. Connectivity between storage and server devices should be done via FC SAN switches via two (2) dedicated redundant fabrics. Storage arrays and SAN switches should be compatible with fabric version GEN 7 or higher support.
The specification devices must have the following features:

- The solution must include redundancy features, such as RAID configurations, dual power supplies, dual controllers, multiple connectivity modules, Redundant dual-sockets.
- Support for Flash (SSD), SAS, NL-SAS drives
- Drive Enclosures supported with the ability to expand with additional enclosures up to 6 PB
- Inline deduplication + compression
- Caching options for tiering
- Supported RAID Configurations: 1/0, 5, 6
- Backend Connectivity: 12 Gb/s SAS (multiple lane options)
- Protocols: Block (FC, iSCSI), File (NFS/SMB), vVols
- Replication, snapshots, thin provisioning, QoS
- All associated licenses should be included for a minimum five (5) years (centralised management console, reporting, capacity, replication, data-hold, retention, encryption, client and all other feature licenses).
- All firmware and software version upgrades should be included for a minimum five (5) years.
- All Hardware must be covered with 5-year warranty with a 6-hour fix.
- Vendor support is mandatory to maintain operational continuity and compliance with data protection regulations.

- Must be able to scale to accommodate future data growth.
- Data Encryption (AES-256) support, with KMIP support
- Single-pane console for monitoring, reporting, analytics, and policy enforcement across all environments.
- Support for immutable backups to protect against ransomware.
- The hardware must be deployed with minimal downtime, requiring a phased implementation plan and comprehensive testing to ensure reliability.
- Any proposed OEMs must be fully supported by the bidder using OEM-certified staff at the equivalent requested certification levels.

13.4 Work Package Special Notes / Terms:

- Provide Documentation (as built and update of existing documents / drawings)
- Asset tag of hardware
- Follow ACSA capitalisation process
- Labelling as per ACSA standards
- Include project management services
- Work will be performed after hours and must be costed accordingly
- Physical installation, configuration and commissioning of work package equipment
- Decommissioning, un-racking, packaging and moving to storeroom of replaced equipment

14.0 Work Package: Shared Storage Solution - Replacement - Specification C

14.1 Short Description

Supply, physically install and configure replacement storage devices that are used for shared workloads and long term storage.

14.2 As-is environment:

The production and DR shared storage environments, utilize Dell Unity storage arrays to provide LUNS to physical servers (HPE Blade System C7000 BL-series) as block storage as well as VMFS datastores to VMware and Hyper-V. The existing shared storage systems currently do not cater for any tiering or archiving functionality. These are flash only devices hosting all the current data. It is connected to 2 x identical 16Gbps local fiber fabrics (Dell Connectrix B6620D switches) hosted at JNB, CPT and DUR. Each of the two data centre rooms per site, has two (2) storage systems to provide for redundancy and failover across the two rooms.

OR Tambo (JNB): 2 x Unity 500F
Cape Town (CPT): 2 x Unity 450F
King Shaka (DUR): 2 x Unity 450F

OR Tambo (JNB) DR: 1 x Unity 450F
Cape Town (CPT) DR: 1 x Unity 450F

14.3 To/be Requirement:

Replace the distributed storage arrays with two (2) centralised shared storage arrays per site, split over 2 rooms and connected via redundant fiber channel fabrics. The two (2) shared storage systems will provide redundancy as well as consolidate all storage into less devices to manage and maintain, only growing the storage capacity as needed. Connectivity between storage and server devices should be done via FC SAN switches via two (2) dedicated redundant fabrics. Storage arrays and SAN switches should be compatible with fabric version GEN 7 or higher support.
The specification devices must have the following features:

- The solution must include redundancy features, such as RAID configurations, dual power supplies, dual controllers, multiple connectivity modules, Redundant dual-sockets.
- Support for Flash (SSD), SAS, NL-SAS drives
- Drive Enclosures supported with the ability to expand with additional enclosures up to 1 PB
- Inline deduplication + compression
- Caching options for tiering
- Supported RAID Configurations: 1/0, 5, 6
- Backend Connectivity: 12 Gb/s SAS (multiple lane options)
- Protocols: Block (FC, iSCSI), File (NFS/SMB), vVols
- Replication, snapshots, thin provisioning, QoS
- All associated licenses should be included for a minimum five (5) years (centralised management console, reporting, capacity, replication, data-hold, retention, encryption, client and all other feature licenses).
- All firmware and software version upgrades should be included for a minimum five (5) years.
- All Hardware must be covered with 5-year warranty with a 6-hour fix.
- Vendor support is mandatory to maintain operational continuity and compliance with data protection regulations.
- Must be able to scale to accommodate future data growth.

- Data Encryption (AES-256) support, with KMIP support
- Single-pane console for monitoring, reporting, analytics, and policy enforcement across all environments.
- Support for immutable backups to protect against ransomware.
- The hardware must be deployed with minimal downtime, requiring a phased implementation plan and comprehensive testing to ensure reliability.
- Any proposed OEMs must be fully supported by the bidder using OEM-certified staff at the equivalent requested certification levels.

14.4 Work Package Special Notes / Terms:

- Provide Documentation (as built and update of existing documents / drawings)
- Asset tag of hardware
- Follow ACSA capitalisation process
- Labelling as per ACSA standards
- Include project management services
- Work will be performed after hours and must be costed accordingly
- Physical installation, configuration and commissioning of work package equipment
- Decommissioning, un-racking, packaging and moving to storeroom of replaced equipment

15.0 Work Package: Shared Storage Solution - Capacity Upgrade - Specification A

15.1 Short Description

Storage system used in Airports Company South Africa are scalable to keep up with capacity demands. Since the devices has a long lifecycle, it requires for additional storage shelves and disks to be added to cater for operational and project requirements.
Supply, physically install and configure additional storage capacity, including expansion shelves and various enterprise drives to expand existing shared storage systems.

15.2 As-is environment:

The production and DR shared storage environments, utilize Dell Unity storage arrays to provide LUNS to physical servers (HPE Blade System C7000 BL-series) as block storage as well as VMFS datastores to VMware and Hyper-V. The existing shared storage systems currently do not cater for any tiering or archiving functionality. These are flash only devices hosting all the current data. It is connected to 2 x identical 16Gbps local fiber fabrics (Dell Connectrix B6620D switches) hosted at JNB, CPT and DUR. Each of the two data centre rooms per site, has two (2) storage systems to provide for redundancy and failover across the two rooms.

OR Tambo (JNB): 2 x Unity 500F
Cape Town (CPT): 2 x Unity 450F
King Shaka (DUR): 2 x Unity 450F

OR Tambo (JNB) DR: 1 x Unity 450F
Cape Town (CPT) DR: 1 x Unity 450F

15.3 To/be Requirement:

The specification devices must have the following features:

- The expansion solution should have a minimum of 50 TB usable storage (or to the closest 1 TB) and should include all required hardware needed to achieve this. This includes expansions shelves, cabling, sfps, etc.
- All associated licenses should be included for a minimum five (5) years (centralised management console, reporting, capacity, replication, data-hold, retention, encryption, client and all other feature licenses).
- All firmware and software version upgrades should be included for a minimum five (5) years.
- All Hardware must be covered with 5-year warranty with a 6-hour fix.
- Vendor support is mandatory to maintain operational continuity and compliance with data protection regulations.
- The solution must include redundancy features, such as RAID configurations, dual power supplies, dual controllers, multiple connectivity modules.
- The hardware must be deployed with minimal downtime, requiring a phased implementation plan and comprehensive testing to ensure reliability.
- Any proposed OEMs must be fully supported by the bidder using OEM-certified staff at the equivalent requested certification levels.

15.4 Work Package Special Notes / Terms:

- Provide Documentation (as built and update of existing documents / drawings)
- Asset tag of hardware

- Follow ACSA capitalisation process
- Labelling as per ACSA standards
- Include project management services
- Work will be performed after hours and must be costed accordingly
- Physical installation, configuration and commissioning of work package equipment
- Decommissioning, un-racking, packaging and moving to storeroom of replaced equipment

16.0 Work Package: Shared Storage Solution - Capacity Upgrade - Specification B

16.1 Short Description

Storage system used in Airports Company South Africa are scalable to keep up with capacity demands. Since the devices has a long lifecycle, it requires for additional storage shelves and disks to be added to cater for operational and project requirements.
Supply, physically install and configure additional storage capacity, including expansion shelves and various enterprise drives to expand existing shared storage systems.

16.2 As-is environment:

The production and DR shared storage environments, utilize Dell Unity storage arrays to provide LUNS to physical servers (HPE Blade System C7000 BL-series) as block storage as well as VMFS datastores to VMware and Hyper-V. The existing shared storage systems currently do not cater for any tiering or archiving functionality. These are flash only devices hosting all the current data. It is connected to 2 x identical 16Gbps local fiber fabrics (Dell Connectrix B6620D switches) hosted at JNB, CPT and DUR. Each of the two data centre rooms per site, has two (2) storage systems to provide for redundancy and failover across the two rooms.

OR Tambo (JNB): 2 x Unity 500F
Cape Town (CPT): 2 x Unity 450F
King Shaka (DUR): 2 x Unity 450F

OR Tambo (JNB) DR: 1 x Unity 450F
Cape Town (CPT) DR: 1 x Unity 450F

16.3 To/be Requirement:

The specification devices must have the following features:

- The expansion solution should have a minimum of 10 TB usable storage (or to the closest 1 TB) and should include all required hardware needed to achieve this. This includes expansions shelves, cabling, sfps, etc.
- All associated licenses should be included for a minimum five (5) years (centralised management console, reporting, capacity, replication, data-hold, retention, encryption, client and all other feature licenses).
- All firmware and software version upgrades should be included for a minimum five (5) years.
- All Hardware must be covered with 5-year warranty with a 6-hour fix.
- Vendor support is mandatory to maintain operational continuity and compliance with data protection regulations.
- The solution must include redundancy features, such as RAID configurations, dual power supplies, dual controllers, multiple connectivity modules.
- The hardware must be deployed with minimal downtime, requiring a phased implementation plan and comprehensive testing to ensure reliability.
- Any proposed OEMs must be fully supported by the bidder using OEM-certified staff at the equivalent requested certification levels.

16.4 Work Package Special Notes / Terms:

- Provide Documentation (as built and update of existing documents / drawings)
- Asset tag of hardware

- Follow ACSA capitalisation process
- Labelling as per ACSA standards
- Include project management services
- Work will be performed after hours and must be costed accordingly
- Physical installation, configuration and commissioning of work package equipment
- Decommissioning, un-racking, packaging and moving to storeroom of replaced equipment

17.0 Work Package: Shared Storage Solution - Capacity Upgrade - Specification C

17.1 Short Description

Storage system used in Airports Company South Africa are scalable to keep up with capacity demands. Since the devices has a long lifecycle, it requires for additional storage shelves and disks to be added to cater for operational and project requirements.
Supply, physically install and configure additional storage capacity, including expansion shelves and various enterprise drives to expand existing shared storage systems.

17.2 As-is environment:

The production and DR shared storage environments utilise Dell Unity storage arrays to provide LUNs to physical servers (HPE BladeSystem C7000 BL-series) as block storage, as well as VMFS datastores to VMware and Hyper-V. The existing shared storage systems currently do not cater for any tiering or archiving functionality. These are flash only devices hosting all the current data. It is connected to 2 x identical 16Gbps local fibre fabrics (Dell Connectrix B6620D switches) hosted at JNB, CPT and DUR. Each of the two data centre rooms per site has two (2) storage systems to provide for redundancy and failover across the two rooms.

OR Tambo (JNB): 2 x Unity 500F
Cape Town (CPT): 2 x Unity 450F
King Shaka (DUR): 2 x Unity 450F

OR Tambo (JNB) DR: 1 x Unity 450F
Cape Town (CPT) DR: 1 x Unity 450F

17.3 To/be Requirement:

The specification devices must have the following features:

- The expansion solution should have a minimum of 1 TB usable storage (or to the closest 1 TB) and should include all required hardware needed to achieve this. This includes expansions shelves, cabling, SFPS, etc.
- All associated licenses should be included for a minimum five (5) years (centralised management console, reporting, capacity, replication, data-hold, retention, encryption, client and all other feature licenses).
- All firmware and software version upgrades should be included for a minimum five (5) years.
- All Hardware must be covered with 5-year warranty with a 6-hour fix.
- Vendor support is mandatory to maintain operational continuity and compliance with data protection regulations.
- The solution must include redundancy features, such as RAID configurations, dual power supplies, dual controllers, multiple connectivity modules.
- The hardware must be deployed with minimal downtime, requiring a phased implementation plan and comprehensive testing to ensure reliability.
- Any proposed OEMs must be fully supported by the bidder using OEM-certified staff at the equivalent requested certification levels.

17.4 Work Package Special Notes / Terms:

- Provide Documentation (as built and update of existing documents / drawings)
- Asset tag of hardware

- Follow ACSA capitalisation process
- Labelling as per ACSA standards
- Include project management services
- Work will be performed after hours and must be costed accordingly
- Physical installation, configuration and commissioning of work package equipment
- Decommissioning, un-racking, packaging and moving to storeroom of replaced equipment

18.0 Work Package: SAN Switch Solution - Replacement - Specification A

18.1 Short Description

To connect compute and storage systems that are highly reliable and flexible, a robust Storage Area Network (SAN) is needed. Airports Company South Africa has SAN fabrics connecting compute and storage systems in multiple rooms within multiple sites. When these devices reach end of life, they need to be replaced with new hardware.
Supply, physically install and configure replacement SAN switches, including SFPs to expand existing connected systems.

18.2 As-is environment:

The current SAN fabrics at JNB, CPT, DUR and PLZ are split into Fabric A and Fabric B and span across data centres. They all utilize the same family model switches to connect the storage systems to the Blade Servers. Each storage system has 2 ports connected from SP-A to Fabric A and 2 ports connected from SP-B to Fabric B. Each Blade Server Enclosure has 3 x fibre connections from Fabric A and 3 x fibre connection from Fabric B. The switches in the same Fabrics are connected between rooms with 3 ISL connections.
All fibre connections are multi-mode, EXCEPT the cross room ISL link, which are single mode.

OR Tambo (JNB):

- Total: 10 x DS-6620B switches
- Room 1
  - 4 x DS-6620B switches in Fabric A (160 ports used, allow for 20% expansion)
- Room 2
  - 4 x DS-6620B switches in Fabric B (158 ports used, allow for 20% expansion)
- DR
  - 1 x DS-6620B switches in Fabric A (20 ports used, allow for 20% expansion)
  - 1 x DS-6620B switches in Fabric B (20 ports used, allow for 20% expansion)

18.3 To/be Requirement:

The replacement fiber channel SAN switches should be compatible with the existing storage arrays and server hardware. It must:

- 1U or 2U rack mountable form factor
- Minimum of 48 ports enabled and licenced with 4 single mode SFP’s for ISLs and 44 multi-mode SFP’s per switch
- Additional ports and SFP’s should be added to match the as-is port requirements for all four (4) fabrics above.
  - Production Fabric A,
  - Production Fabric B,
  - DR Fabric A,
  - DR Fabric B
- SFP’s should be capable of 64Gb/s or higher speeds. Port should be backward compatible with 32Gb/s or 16Gb/s SFPs
- Multiple built-in redundancies: dual power supplies, dual fans with front -to-rear and rear-to-front airflow options, dual processors (ASICs).
- Support Fibre Channel Gen 7 or later

- All active ports should be fully licensed for all supported features
- Ports should support trunking
- Ports should support single mode and multimode SFPs
- The switches should support a central management system, but also have the option of direct management via web and ssh interface
- Supported port types:
  - E_Port, EX_Port, F_Port, M_Port
  - Access Gateway mode: F_Port and NPIV-enabled N_Port
- Security Features:
  - DH-CHAP (between switches and end devices); FCAP switch authentication; HTTPS; IP filtering; LDAP; Port Binding; RADIUS; TACACS+; user-defined Role-Based Access Control (RBAC)
- Fabric Services
  - BB Credit Recovery; Advanced Zoning (Default Zoning, Port/WWN Zoning, Peer Zoning); Congestion Signaling; Dynamic Path Selection (DPS); Extended Fabrics; Fabric Performance Impact Notification (FPIN); Fabric Vision; FDMI; FICON CUP; Flow Vision; F_Port Trunking; FSPF; Integrated Routing; ISL Trunking; Management Server; Name Server; NPIV; NTP v3; Port Decommission/Fencing; QoS; Registered State Change Notification (RSCN); Slow Drain Device Quarantine (SDDQ); Target-Driven Zoning; Traffic Optimizer; Virtual Fabrics (Logical Switch, Logical Fabric); VMID+ and AppServer
- All associated licenses should be included for a minimum five (5) years (centralised management console, reporting, capacity, replication, data-hold, retention, encryption, client and all other feature licenses).
- All firmware and software version upgrades should be included for a minimum five (5) years.
- All Hardware must be covered with 5-year warranty with a 6-hour fix.
- Vendor support is mandatory to maintain operational continuity and compliance with data protection regulations.
- The solution must include redundancy features, such as RAID configurations, dual power supplies, dual controllers, multiple connectivity modules.
- The hardware must be deployed with minimal downtime, requiring a phased implementation plan and comprehensive testing to ensure reliability.
- Any proposed OEMs must be fully supported by the bidder using OEM-certified staff at the equivalent requested certification levels.

19.0 Work Package: SAN Switch Solution - Replacement - Specification B

19.1 Short Description

To connect compute and storage systems that are highly reliable and flexible, a robust Storage Area Network (SAN) is needed. Airports Company South Africa has SAN fabrics connecting compute and storage systems in multiple rooms within multiple sites. When these devices reach end of life, they need to be replaced with new hardware.
Supply, physically install and configure replacement SAN switches, including SFPs to expand existing connected systems.

19.2 As-is environment:

The current SAN fabrics at JNB, CPT, DUR and PLZ are split into Fabric A and Fabric B and span across data centres. They all utilize the same family model switches to connect the storage systems to the Blade Servers. Each storage system has 2 ports connected from SP-A to Fabric A and 2 ports connected from SP-B to Fabric B. Each Blade Server Enclosure has 3 x fibre connections from Fabric A and 3 x fibre connection from Fabric B. The switches in the same Fabrics are connected between rooms with 3 ISL connections.
All fibre connections are multi-mode, EXCEPT the cross room ISL link, which are single mode.

Cape Town (CPT):

- Total: 6 x DS-6620B switches
- Room 1
  - 2 x DS-6620B switches in Fabric A (49 ports used, allow for 20% expansion)
- Room 2
  - 2 x DS-6620B switches in Fabric B (48 ports used, allow for 20% expansion)
- DR
  - 1 x DS-6620B switches in Fabric A (15 ports used, allow for 20% expansion)
  - 1 x DS-6620B switches in Fabric B (15 ports used, allow for 20% expansion)

19.3 To/be Requirement:

The replacement fiber channel SAN switches should be compatible with the existing storage arrays and server hardware. It must:

- 1U or 2U rack mountable form factor
- Minimum of 48 ports enabled and licenced with 4 single mode SFP’s for ISLs and 44 multi-mode SFP’s per switch
- Additional ports and SFP’s should be added to match the as-is port requirements for all four (4) fabrics above.
  - Production Fabric A,
  - Production Fabric B,
  - DR Fabric A,
  - DR Fabric B
- SFP’s should be capable of 64Gb/s or higher speeds. Port should be backward compatible with 32Gb/s or 16Gb/s SFPs
- Multiple built-in redundancies: dual power supplies, dual fans with front -to-rear and rear-to-front airflow options, dual processors (ASICs).
- Support Fibre Channel Gen 7 or later

- All active ports should be fully licensed for all supported features
- Ports should support trunking
- Ports should support single mode and multimode SFPs
- The switches should support a central management system, but also have the option of direct management via web and ssh interface
- Supported port types:
  - E_Port, EX_Port, F_Port, M_Port
  - Access Gateway mode: F_Port and NPIV-enabled N_Port
- Security Features:
  - DH-CHAP (between switches and end devices); FCAP switch authentication; HTTPS; IP filtering; LDAP; Port Binding; RADIUS; TACACS+; user-defined Role-Based Access Control (RBAC)
- Fabric Services
  - BB Credit Recovery; Advanced Zoning (Default Zoning, Port/WWN Zoning, Peer Zoning); Congestion Signaling; Dynamic Path Selection (DPS); Extended Fabrics; Fabric Performance Impact Notification (FPIN); Fabric Vision; FDMI; FICON CUP; Flow Vision; F_Port Trunking; FSPF; Integrated Routing; ISL Trunking; Management Server; Name Server; NPIV; NTP v3; Port Decommission/Fencing; QoS; Registered State Change Notification (RSCN); Slow Drain Device Quarantine (SDDQ); Target-Driven Zoning; Traffic Optimizer; Virtual Fabrics (Logical Switch, Logical Fabric); VMID+ and AppServer
- All associated licenses should be included for a minimum five (5) years (centralised management console, reporting, capacity, replication, data-hold, retention, encryption, client and all other feature licenses).
- All firmware and software version upgrades should be included for a minimum five (5) years.
- All Hardware must be covered with 5-year warranty with a 6-hour fix.
- Vendor support is mandatory to maintain operational continuity and compliance with data protection regulations.
- The solution must include redundancy features, such as RAID configurations, dual power supplies, dual controllers, multiple connectivity modules.
- The hardware must be deployed with minimal downtime, requiring a phased implementation plan and comprehensive testing to ensure reliability.
- Any proposed OEMs must be fully supported by the bidder using OEM-certified staff at the equivalent requested certification levels.

20.0 Work Package: SAN Switch Solution - Replacement - Specification C

20.1 Short Description

To connect compute and storage systems that are highly reliable and flexible, a robust Storage Area Network (SAN) is needed. Airports Company South Africa has SAN fabrics connecting compute and storage systems in multiple rooms within multiple sites. When these devices reach end of life, they need to be replaced with new hardware.
Supply, physically install and configure replacement SAN switches, including SFPs to expand existing connected systems.

20.2 As-is environment:

The current SAN fabrics at JNB, CPT, DUR and PLZ are split into Fabric A and Fabric B and span across data centres. They all utilize the same family model switches to connect the storage systems to the Blade Servers. Each storage system has 2 ports connected from SP-A to Fabric A and 2 ports connected from SP-B to Fabric B. Each Blade Server Enclosure has 3 x fibre connections from Fabric A and 3 x fibre connection from Fabric B. The switches in the same Fabrics are connected between rooms with 3 ISL connections.
All fibre connections are multi-mode, EXCEPT the cross room ISL link, which are single mode.

King Shaka (DUR):

- Total: 4 x DS-6620B switches
- Room 1
  - 2 x DS-6620B switches in Fabric A (33 ports used, allow for 20% expansion)
- Room 2
  - 2 x DS-6620B switches in Fabric B (48 ports used, allow for 20% expansion)

20.3 To/be Requirement:

The replacement fiber channel SAN switches should be compatible with the existing storage arrays and server hardware. It must:

- 1U or 2U rack mountable form factor
- Minimum of 48 ports enabled and licenced with 4 single mode SFP's for ISLs and 44 multi-mode SFP's per switch
- Additional ports and SFP's should be added to match the as-is port requirements for both (2) fabrics above.
  - Production Fabric A,
  - Production Fabric B,
- SFP's should be capable of 64Gb/s or higher speeds. Port should be backward compatible with 32Gb/s or 16Gb/s SFPs
- Multiple built-in redundancies: dual power supplies, dual fans with front -to-rear and rear-to-front airflow options, dual processors (ASICs).
- Support Fibre Channel Gen 7 or later
- All active ports should be fully licensed for all supported features
- Ports should support trunking
- Ports should support single mode and multimode SFPs
- The switches should support a central management system, but also have the option of direct management via web and ssh interface
- Supported port types:
  - E_Port, EX_Port, F_Port, M_Port

  - Access Gateway mode: F_Port and NPIV-enabled N_Port
- Security Features:
  - DH-CHAP (between switches and end devices); FCAP switch authentication; HTTPS; IP filtering; LDAP; Port Binding; RADIUS; TACACS+; user-defined Role-Based Access Control (RBAC)
- Fabric Services
  - BB Credit Recovery; Advanced Zoning (Default Zoning, Port/WWN Zoning, Peer Zoning); Congestion Signaling; Dynamic Path Selection (DPS); Extended Fabrics; Fabric Performance Impact Notification (FPIN); Fabric Vision; FDMI; FICON CUP; Flow Vision; F_Port Trunking; FSPF; Integrated Routing; ISL Trunking; Management Server; Name Server; NPIV; NTP v3; Port Decommission/Fencing; QoS; Registered State Change Notification (RSCN); Slow Drain Device Quarantine (SDDQ); Target-Driven Zoning; Traffic Optimizer; Virtual Fabrics (Logical Switch, Logical Fabric); VMID+ and AppServer
- All associated licenses should be included for a minimum five (5) years (centralised management console, reporting, capacity, replication, data-hold, retention, encryption, client and all other feature licenses).
- All firmware and software version upgrades should be included for a minimum five (5) years.
- All Hardware must be covered with 5-year warranty with a 6-hour fix.
- Vendor support is mandatory to maintain operational continuity and compliance with data protection regulations.
- The solution must include redundancy features, such as RAID configurations, dual power supplies, dual controllers, multiple connectivity modules.
- The hardware must be deployed with minimal downtime, requiring a phased implementation plan and comprehensive testing to ensure reliability.
- Any proposed OEMs must be fully supported by the bidder using OEM-certified staff at the equivalent requested certification levels.

21.0 Work Package: SAN Switch Solution - Capacity Upgrade - Specification A

21.1 Short Description

Supply, physically install, license and configure additional SAN switch ports, including SFPs to expand existing connected systems.

21.2 As-is environment:

The current SAN switches (Dell Connectrix DS-6620B) are not fully populated or licensed and can be expanded further.

21.3 To/be Requirement:

Add additional port licenses with accompanying SFP's for additional connectivity on the existing SAN fabric switches.
It must:

- Include single-mode SFP's for the same number of ports added
- SFP's should be capable of 32Gb/s or higher speeds. Port should be backward compatible with 16Gb/s SFPs
- Support Fibre Channel Gen 6 or later
- All active ports should be fully licensed for all supported features
- Ports should support trunking
- All associated licenses should be included for a minimum five (5) years (centralised management console, reporting, capacity, replication, data-hold, retention, encryption, client and all other feature licenses).
- All firmware and software version upgrades should be included for a minimum five (5) years.
- All Hardware must be covered with 5-year warranty with a 6-hour fix.
- Vendor support is mandatory to maintain operational continuity and compliance with data protection regulations.
- The solution must include redundancy features, such as RAID configurations, dual power supplies, dual controllers, multiple connectivity modules.
- The hardware must be deployed with minimal downtime, requiring a phased implementation plan and comprehensive testing to ensure reliability.
- Any proposed OEMs must be fully supported by the bidder using OEM-certified staff at the equivalent requested certification levels.

22.0 Work Package: SAN Switch Solution - Capacity Upgrade - Specification B

22.1 Short Description

Supply, physically install, license and configure additional SAN switch ports, including SFPs to expand existing connected systems.

22.2 As-is environment:

The current SAN switches (Dell Connectrix DS-6620B) are not fully populated or licensed and can be expanded further.

22.3 To/be Requirement:

Add additional port licenses with accompanying SFP's for additional connectivity on the existing SAN fabric switches.
It must:

- Include multi-mode SFP's for the same number of ports added
- SFP's should be capable of 32Gb/s or higher speeds. Port should be backward compatible with 16Gb/s SFPs
- Support Fibre Channel Gen 6 or later
- All active ports should be fully licensed for all supported features
- Ports should support trunking
- All associated licenses should be included for a minimum five (5) years (centralised management console, reporting, capacity, replication, data-hold, retention, encryption, client and all other feature licenses).
- All firmware and software version upgrades should be included for a minimum five (5) years.
- All Hardware must be covered with 5-year warranty with a 6-hour fix.
- Vendor support is mandatory to maintain operational continuity and compliance with data protection regulations.
- The solution must include redundancy features, such as RAID configurations, dual power supplies, dual controllers, multiple connectivity modules.
- The hardware must be deployed with minimal downtime, requiring a phased implementation plan and comprehensive testing to ensure reliability.
- Any proposed OEMs must be fully supported by the bidder using OEM-certified staff at the equivalent requested certification levels.

23.0 Work Package: Backup Monitoring, Management and Reporting Tools

23.1 Short Description

Airports Company South Africa manages 9 airports and a head office located at OR Tambo Aviation Park. All of these sites have a combination of backups, storage and SAN networking which requires monitoring and management on a 24/7/365 basis. For this reason, troubleshooting and management tools require to be kept up to date or refreshed/replaced throughout the product lifecycles.
Supply, install, license and configure Backup Monitoring, Management and Reporting Tools to optimised operational tasks and reporting.

23.2 As-is environment:

Various built in tools are available to assist with managing the environments. Gathering and coordinating health checks and reports in this way does not make sense across multiple backup clients, storage arrays and SAN switches. Centralised monitoring and reporting provide this in a quick and efficient way as well as global tending and analysis functions. These are listed below as it pertains to the various areas:

- Data Protection (Backups & Replication)
  - Data Protection Advisor (DPA)
  - Data Protection Central (DPC)
  - Data Domain Management Center (DDMC)
- Multi-monitoring / management tools
  - Dell Storage Resource Manager (Dell SRM)
  - Dell AIOps (formerly CloudIQ)

23.3 To/be Business Requirements

Provide a single-pane, one-tool solution to monitor, manage and report on the existing backup products. Provided OEM validated configurations. Configure the backup and backup storage equipment within these tools with documented configurations.
It should:

- Multi-vendor / multi-platform support
- Global dashboard with drill-down functionality
- Federated/multi-tenant views
- Proactive anomaly detection
- Intelligent alerting with noise suppression & correlation
- Capacity forecasting & trend analysis
- Success/failure rates per policy, application, server, job
- Restore job tracking & success reporting
- RPO/RTO compliance reporting
- Cost allocation & chargeback/showback reports
- Long-term retention compliance reporting
- Audit trails of all configuration changes
- Customizable regulatory reports (out-of-the-box templates)
- Customizable historical data retention
- Root-cause analysis with timeline correlation
- Automated & Scheduled Email Reporting
- Export of reports to various formats including PDF, CSV, HTML, Excel

- All associated licenses should be included for a minimum five (5) years (centralised management console, reporting, capacity, replication, data-hold, retention, encryption, client and all other feature licenses).
- All firmware and software version upgrades should be included for a minimum five (5) years.
- All Hardware must be covered with 5-year warranty with a 6-hour fix.
- Vendor support is mandatory to maintain operational continuity and compliance with data protection regulations.
- The solution must include redundancy features, such as RAID configurations, dual power supplies, dual controllers, multiple connectivity modules.
- The hardware must be deployed with minimal downtime, requiring a phased implementation plan and comprehensive testing to ensure reliability.
- Any proposed OEMs must be fully supported by the bidder using OEM-certified staff at the equivalent requested certification levels.

24.0 Work Package: Storage Monitoring, Management and Reporting Tools

24.1 Short Description

Airports Company South Africa manages 9 airports and a head office located at OR Tambo Aviation Park. All of these sites have a combination of backups, storage and SAN networking which requires monitoring and management on a 24/7/365 basis. For this reason, troubleshooting and management tools require to be kept up to date or refreshed/replaced throughout the product lifecycles.
Supply, install, license and configure Storage Monitoring, Management and Reporting Tools to optimised operational tasks and reporting.

24.2 As-is environment:

Various built in tools are available to assist with managing the environments. Gathering and coordinating health checks and reports in this way does not make sense across multiple backup clients, storage arrays and SAN switches. Centralised monitoring and reporting provide this in a quick and efficient way as well as global tending and analysis functions. These are listed below as it pertains to the various areas:

- Data Storage (SAN Storage & Networking)
    - Unisphere Central
    - AppSync
    - PowerPath
- Multi-monitoring / management tools
    - Dell Storage Resource Manager (Dell SRM)
    - Dell AIOps (formerly CloudIQ)

24.3 To/be Business Requirements

Provide a single-pane, one-tool solution to monitor, manage and report on the existing SAN storage products. Provided OEM validated configurations. Configure the storage equipment within these tools with documented configurations.
It should:

- Multi-vendor / multi-platform support
- Global dashboard with drill-down functionality
- Federated/multi-tenant views
- End-to-end topology mapping (host → fabric → array → LUN/volume → pool)
- AI-driven anomaly detection & baseline deviation
- Role-based access control (RBAC) Audit logging of all actions Encryption and D@RE status visibility
- Switch port statistics, zoning, ISL/trunk utilization (when integrated with Fabric OS)
- Smart alerting with suppression, correlation, and escalation (email, SNMP, ServiceNow)
- Capacity forecasting & trend analysis
- Automated provisioning, zoning, replication, snapshots
- Storage consumption & cost allocation by department, application, tenant Showback/chargeback reports including cloud tier costs
- Audit trails of all configuration changes
- Customizable historical data retention
- Root-cause analysis with timeline correlation
- Automated & Scheduled Email Reporting

- Export of reports to various formats including PDF, CSV, HTML, Excel
- All associated licenses should be included for a minimum five (5) years (centralised management console, reporting, capacity, replication, data-hold, retention, encryption, client and all other feature licenses).
- All firmware and software version upgrades should be included for a minimum five (5) years.
- All Hardware must be covered with 5-year warranty with a 6-hour fix.
- Vendor support is mandatory to maintain operational continuity and compliance with data protection regulations.
- The solution must include redundancy features, such as RAID configurations, dual power supplies, dual controllers, multiple connectivity modules.
- The hardware must be deployed with minimal downtime, requiring a phased implementation plan and comprehensive testing to ensure reliability.
- Any proposed OEMs must be fully supported by the bidder using OEM-certified staff at the equivalent requested certification levels.

25.0 Work Package: SAN Storage Network Monitoring, Management and Reporting Tools

25.1 Short Description

Airports Company South Africa manages 9 airports and a head office located at OR Tambo Aviation Park. All of these sites have a combination of backups, storage and SAN networking which requires monitoring and management on a 24/7/365 basis. For this reason, troubleshooting and management tools require to be kept up to date or refreshed/replaced throughout the product lifecycles.
Supply, install, license and configure SAN Storage Network Monitoring, Management and Reporting Tools to optimised operational tasks and reporting.

25.2 As-is environment:

Various built in tools are available to assist with managing the environments. Gathering and coordinating health checks and reports in this way does not make sense across multiple backup clients, storage arrays and SAN switches. Centralised monitoring and reporting provide this in a quick and efficient way as well as global tending and analysis functions. These are listed below as it pertains to the various areas:

- Data Storage (SAN Storage & Networking)
  - Connectrix SANnav Portal
- Multi-monitoring / management tools
  - Dell Storage Resource Manager (Dell SRM)
  - Dell AIOps (formerly CloudIQ)

25.3 To/be Business Requirements

Provide a single-pane, one-tool solution to monitor, manage and report on the existing SAN storage products. Provided OEM validated configurations. Configure the storage equipment within these tools with documented configurations.
It should:

- Multi-vendor / multi-platform support
- Global dashboard with drill-down functionality
- Federated/multi-tenant views
- End-to-end topology mapping (host → fabric → array → LUN/volume → pool)
- AI-driven anomaly detection & baseline deviation
- Role-based access control (RBAC) Audit logging of all actions Encryption and D@RE status visibility
- Switch port statistics, zoning, ISL/trunk utilization (when integrated with Fabric OS)
- Smart alerting with suppression, correlation, and escalation (email, SNMP, ServiceNow)
- Capacity forecasting & trend analysis
- Automated provisioning, zoning, replication, snapshots
- Storage consumption & cost allocation by department, application, tenant Showback/chargeback reports including cloud tier costs
- Audit trails of all configuration changes
- Customizable historical data retention
- Root-cause analysis with timeline correlation
- Automated & Scheduled Email Reporting
- Export of reports to various formats including PDF, CSV, HTML, Excel

- All associated licenses should be included for a minimum five (5) years (centralised management console, reporting, capacity, replication, data-hold, retention, encryption, client and all other feature licenses).
- All firmware and software version upgrades should be included for a minimum five (5) years.
- All Hardware must be covered with 5-year warranty with a 6-hour fix.
- Vendor support is mandatory to maintain operational continuity and compliance with data protection regulations.
- The solution must include redundancy features, such as RAID configurations, dual power supplies, dual controllers, multiple connectivity modules.
- The hardware must be deployed with minimal downtime, requiring a phased implementation plan and comprehensive testing to ensure reliability.
- Any proposed OEMs must be fully supported by the bidder using OEM-certified staff at the equivalent requested certification levels.

26.0 Work Package: Cyber Recovery Solution

26.1 Short Description

Cyber recovery is essential for enterprises to quickly restore critical systems and data after cyberattacks like ransomware or breaches. It minimizes downtime, protects revenue, ensures compliance, and maintains customer trust. Effective cyber recovery strategies safeguard against further compromise, maintain data integrity, and support compliance with stringent regulatory requirements. By prioritizing cyber recovery, enterprises enhance resilience against evolving cyber threats, mitigate reputational damage, and ensure business continuity in an increasingly hostile digital landscape.

26.2 As-is environment:

Currently, the organization relies solely on traditional backup systems for data recovery, lacking a dedicated cyber recovery solution. This approach is insufficient to address the sophisticated and evolving cyber threats facing modern enterprises, such as ransomware, advanced persistent threats, or insider attacks. A comprehensive cyber recovery solution is imperative to ensure rapid, secure restoration of critical systems and data following a cyber incident. Unlike basic backups, a robust cyber recovery framework incorporates isolated recovery environments, immutable data storage, and advanced threat detection to prevent reinfection and ensure data integrity. Implementing such a solution minimizes operational downtime, protects financial performance, and ensures compliance with stringent regulatory requirements.

26.3 To/be Business Requirements

Provide a cyber recovery solution that will have minimal disruption to ongoing operations, supported by a phased deployment plan, comprehensive staff training, and regular updates to address evolving cyber threats. The solution must include the following requirements:

- **Isolated Recovery Environment:** A secure, air-gapped or logically isolated environment to enable clean restoration of data and systems, preventing reinfection from compromised networks or malware persistence.
- **Immutable Data Storage:** Write-once, read-many (WORM) storages for backups to protect against unauthorized modification or deletion by ransomware or malicious actors.
- **High Availability and Scalability:** The solution must support high-speed recovery to minimize downtime, with scalable storage and processing capacity to accommodate current and future data volumes across enterprise operations.
- **Automated Recovery Processes**: Automated workflows for backup validation, restoration testing, and system recovery to reduce human error and accelerate response times during a cyber incident.
- **Advanced Threat Detection and Monitoring**: Integrated capabilities to detect anomalies, validate backup integrity, and monitor for potential threats within the recovery environment to ensure clean restores.
- **Encryption Standards:** End-to-end encryption (AES-256 or higher) for data in transit and at rest to safeguard sensitive information during storage and recovery processes.
- **Multi-Layered Access Controls:** Robust authentication mechanisms, including multi-factor authentication (MFA) and role-based access controls (RBAC), to restrict access to the recovery environment and prevent unauthorized interference.

- **Regular Testing and Validation:** Scheduled, automated testing of recovery processes to verify data integrity, system functionality, and readiness, ensuring confidence in restoration capabilities under real-world conditions.
- **Compliance Support:** Features to align with regulatory requirements (e.g., GDPR, HIPAA, CCPA), including audit trails, data retention policies, and reporting capabilities to demonstrate compliance during audits.
- **Integration with Existing Infrastructure:** Seamless compatibility with current backup systems, enterprise applications, and hybrid cloud environments to ensure cohesive operation without disrupting existing workflows.
- **Disaster Recovery Alignment:** Coordination with broader disaster recovery plans, including offsite storage and geographic redundancy, to protect against physical and logical disruptions.
- **24/7 Support and Incident Response:** Access to round-the-clock technical support and a defined incident response framework to assist with recovery operations during a cyber crisis.
- All associated licenses should be included for a minimum five (5) years (centralised management console, reporting, capacity, replication, data-hold, retention, encryption, client and all other feature licenses).
- All firmware and software version upgrades should be included for a minimum five (5) years.
- All Hardware must be covered with 5-year warranty with a 6-hour fix.
- Vendor support is mandatory to maintain operational continuity and compliance with data protection regulations.
- The solution must include redundancy features, such as RAID configurations, dual power supplies, dual controllers, multiple connectivity modules.
- The hardware must be deployed with minimal downtime, requiring a phased implementation plan and comprehensive testing to ensure reliability.
- Any proposed OEMs must be fully supported by the bidder using OEM-certified staff at the equivalent requested certification levels.

26.4 Work Package Special Notes / Terms:

- Provide Documentation (as built and update of existing documents / drawings)
- Asset tag of hardware
- Follow ACSA capitalisation process
- Labelling as per ACSA standards
- Include project management services
- Work will be afterhours and must be costed accordingly
- Physical installation, configuration and commissioning of work package equipment
- Decommissioning, unracking, packaging and moving to storeroom of replaced equipment

27.0 Work Package: Microsoft 365 (Formerly Office 365) Cloud Backups

27.1 Short Description

Airports Company South Africa has migrated the Exchange, SharePoint, OneDrive and Teams services from on-prem to Microsoft 365 cloud. The Shared Responsibility Model notes that Microsoft ensures the security of the cloud. This includes keeping the infrastructure running, protecting against hardware failures, and maintaining uptime for services like Microsoft 365. The client (ACSA) is responsible for what happens inside the cloud. This means securing and backing up your own data, managing user access, and ensuring compliance with regulations.
This work package aims to provide a backup solution for all Microsoft 365 workloads:

- Exchange Online – Emails, contacts, calendars, and tasks.
- SharePoint Online – Sites, libraries, and lists.
- OneDrive for Business – Files and folders.
- Microsoft Teams – Conversations, files, and metadata.

27.2 As-is environment:

Currently, ACSA does not have a dedicated backup solution in place to comprehensively protect its Microsoft 365 workloads. This leaves critical business data vulnerable to accidental deletion, cyber threats, and compliance risks due to Microsoft's limited native retention policies.

27.3 To/be Business Requirements

Deploying a comprehensive Cloud Data Protection solution, will align ACSA’s strategic objectives ensuring business continuity, regulatory compliance, and cyber resilience. A secure and reliable backup solution that will mitigate operational risks and enhance data governance. This will ensure protecting critical business data, ensuring uninterrupted operations, and meeting compliance mandates. The solution should provide for the following:

- Comprehensive Backup – Protecting Exchange Online, SharePoint, OneDrive, and Teams with automated backups and granular recovery.
- Instant Recovery – Restore entire accounts or individual files, emails, and Teams messages instantly with point-in-time recovery.
- Ransomware Protection – Immutable backups prevent unauthorized deletion or encryption by cybercriminals. Air-gapped and encrypted storage to provide an additional layer of security.
- Flexible Storage Options – Backup to Azure, AWS, or private cloud, optimizing costs and security.
- Compliance & Audit Readiness – Custom retention policies, legal hold ensures regulatory compliance.
- Cost-Efficient & Scalable – Expansion capability to grow as the infrastructure requirements grow with automated storage tiering for optimized costs.
- Easy Management & Automation – Web-based console, automated scheduling, and real-time reporting for simplified IT operations.
- All associated licenses should be included for a minimum five (5) years (centralised management console, reporting, capacity, replication, data-hold, retention, encryption, client and all other feature licenses).
- All firmware and software version upgrades should be included for a minimum five (5) years.
- All Hardware must be covered with 5-year warranty with a 6-hour fix.

- Vendor support is mandatory to maintain operational continuity and compliance with data protection regulations.
- The solution must include redundancy features, such as RAID configurations, dual power supplies, dual controllers, multiple connectivity modules.
- The hardware must be deployed with minimal downtime, requiring a phased implementation plan and comprehensive testing to ensure reliability.
- Any proposed OEMs must be fully supported by the bidder using OEM-certified staff at the equivalent requested certification levels.

27.4 Work Package Special Notes / Terms:

- Provide Documentation (as built and update of existing documents / drawings)
- Asset tag of hardware
- Follow ACSA capitalisation process
- Labelling as per ACSA standards
- Include project management services
- Work will be afterhours and must be costed accordingly
- Physical installation, configuration and commissioning of work package equipment
- Decommissioning, unracking, packaging and moving to storeroom of replaced equipment

28.0 Work Package: Disaster Recovery Storage Solution

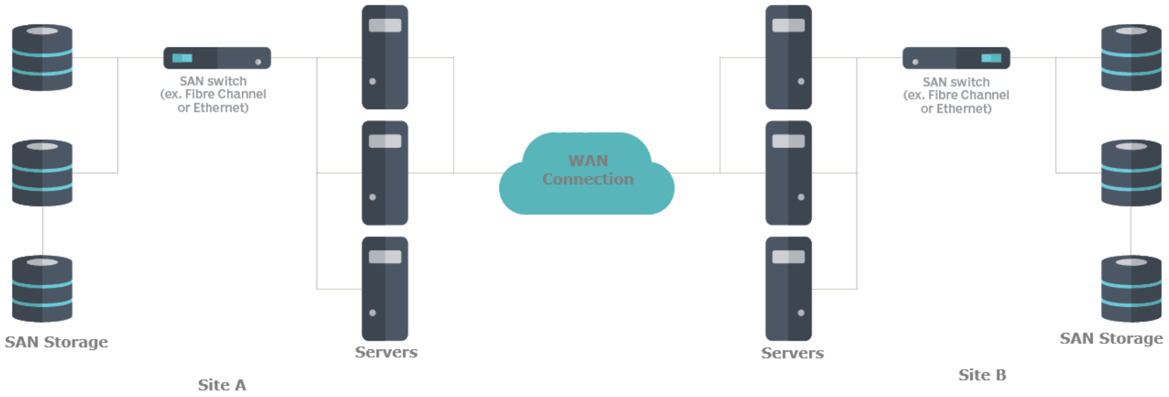
28.1 Short Description

ACSA has identified disaster recovery as an extremely important business objective as such has ensured that disaster recovery hardware and software is in place and kept up to date with production system.

Cape Town International Airport (CIA) was designated as the official disaster recovery site for OR Tambo International Airport (JNB) and King Shaka International Airport (DUR) OR Tambo International Airport (JNB) will be the disaster recovery site for Cape Town International Airport (CIA). This means that both JNB and CIA have disaster recovery hardware and capabilities.

28.2 As is environment

Both sites have a duplicate disaster recovery design. This consists of a centralised storage array utilising FC SAN switches to connect to Blade Servers.



The solution consists of the following:

Site	Make	Model Number
JNB	RecoverPoint	Gen6 Server
JNB	RecoverPoint	Gen6 Server
JNB	Unity	Unity 450F
CPT	RecoverPoint	Gen6 Server
CPT	RecoverPoint	Gen6 Server
CPT	Unity	Unity 450F

28.3 To/be Business Requirements

At OR Tambo International Airport (JNB) and Cape Town International Airport (CIA), replace the existing replication DR devices, SAN storage array and FC SAN switches with an appropriate solution that will perform enterprise Disaster Recovery functions. These can be physical or virtual devices. Note that if a virtual solution is presented, the underlying hardware for this needs to be included in the proposal.
It should:

- Provide Continuous or Near-Continuous Data Replication: Block-level (journal-based) or hypervisor-level replication with RPOs of seconds to minutes. Critical for minimizing data loss.

- Automated Failover & Failback: One-click or fully scripted orchestration of VM failover (power-on in correct order, re-IP, DNS update). Failback with delta sync after cleanup. Reduces MTTR from days to minutes/hours.
- Application-Consistent & Crash-Consistent Protection: Quiescing guest OS (VSS for Windows, VMware Tools quiesce) for databases (SQL, Oracle, Exchange) and crash-consistent for others. Prevents corrupted VMs after recovery.
- Recovery Point Objectives (RPO) Flexibility: Configurable per-VM or per-protection-group (seconds to hours). Journal-based solutions retain multiple historical points (30 days+ of any-point-in-time recovery).
- Recovery Time Objectives (RTO) Flexibility: Parallel VM boot, network virtualization, and automation to meet SLAs for critical applications.
- Non-Disruptive Testing & Compliance Audits: Isolated “bubble” network or sandbox testing of failover without impacting production or replication stream. Generates audit reports proving recoverability.
- WAN Optimization & Bandwidth Throttling: Compression, deduplication, encryption, and scheduling/throttling to minimize impact on expensive remote fiber or IP links.
- Network Virtualization & Automation: Automatic re-IP, MAC preservation or rewrite, DNS updates, route injection, and integration with load balancers.
- Multi-Site & Many-to-One Topologies: Support for active-active, active-passive, or many-to-one (multiple prod sites → one DR site).
- Integration with Hypervisor Native Tools: Deep integration with vCenter/ESXi (VMware SRM + vSphere Replication or third-party storage APIs), Hyper-V Replica enhancements, or AHV protection.
- Self-Service & Role-Based Access: Portal for application owners to initiate test/dev clones or actual failover (with approval workflows).
- Ransomware & Cyber Recovery Features: Immutable recovery points, air-gapped logical isolation, anomaly detection, and clean-room recovery environments.
- Automated Documentation & Runbooks: Generates up-to-date recovery runbooks, dependency mapping, and auditable compliance reports.
- Scalability & Performance: Ability to protect thousands of VMs with minimal overhead on production hosts (<5% CPU/RAM).
- Hybrid & Cloud Bursting: Ability to fail over on-prem VMs to AWS, Azure or other cloud storage as the remote site.
- All associated licenses should be included for a minimum five (5) years (centralised management console, reporting, capacity, replication, data-hold, retention, encryption, client and all other feature licenses).
- All firmware and software version upgrades should be included for a minimum five (5) years.
- All Hardware must be covered with 5-year warranty with a 6-hour fix.
- Vendor support is mandatory to maintain operational continuity and compliance with data protection regulations.
- The solution must include redundancy features, such as RAID configurations, dual power supplies, dual controllers, multiple connectivity modules.
- The hardware must be deployed with minimal downtime, requiring a phased implementation plan and comprehensive testing to ensure reliability.
- Any proposed OEMs must be fully supported by the bidder using OEM-certified staff at the equivalent requested certification levels.

28.4 Work Package Special Notes / Terms:

- Provide Documentation (as built and update of existing documents / drawings)

- Asset tag of hardware
- Follow ACSA capitalisation process
- Labelling as per ACSA standards
- Include project management services
- Work will be afterhours and must be costed accordingly
- Physical installation, configuration and commissioning of work package equipment
- Decommissioning, unracking, packaging and moving to storeroom of replaced equipment

29.0 Work Package: General Supply

29.1 Short Description

From time to time there might be items required that do not form part of the above work packages. This section defines those items.
A list of general supply items not covered in any of the other work packages:

Category	Item Description	UOM	QTY
	Single, dual or quad port 10G Base-T	Each	1
	Single, dual or quad port 10G SFP+	Each	1
	Single, dual or quad port 10/25/100G SFP28	Each	1
	Single, dual or quad port 100G QSFP	Each	1
	Single, dual or quad port 32Gb/64Gb/128Gb FC HBA	Each	1
Data Storage	Four-Port 16 Gb/s Fibre Channel Module or faster	Each	1
	Four-Port 1 GBASE-T Module or faster	Each	1
	Four-Port 10 GBASE-T Module or faster	Each	1
	Two-Port 10 Gb/s Optical Module or faster	Each	1
	Four-Port 10 Gb/s Optical Module or faster	Each	1
	Four-Port 12 Gb/s SAS Module or faster	Each	1
	2.5” Flash or SSD / SAS Drive Disk Array Enclosure (DAE) or Disk Shelf (SAS or Fibre Channel 6/12/24Gbps)	Each	1
	3.5” NL-SAS Drive Disk Array Enclosure (DAE) or Disk Shelf (SAS or Fibre Channel 6/12/24Gbps)	Each	1
	2.5” Flash or SSD Drive: Sizes vary from 100 GB to 16 TB or nearest equivalent	Each	1
	2.5” SAS 15,000 rpm Drive: Sizes vary from 100 GB to 16 TB or larger	Each	1
	2.5” SAS 10,000 rpm Drive: Sizes vary from 100 GB to 16 TB or larger	Each	1
	3.5” SAS 15,000 rpm Drive: Sizes vary from 100 GB to 16 TB or larger	Each	1
	3.5” SAS 10,000 rpm Drive: Sizes vary from 100 GB to 16 TB or larger	Each	1
	3.5” NL-SAS 7,200 rpm Drive: Sizes vary from 100 GB to 16 TB or larger	Each	1
Software	Data Protection (Backup) Software: This includes management console, main application, replication, reporting and archiving function	Each	1
	Data Storage Software: This includes synchronization, management, monitoring & reporting function	Each	1
	Backup & DR Replication Software: This includes replicating LUNs and/or selected virtual data stores and/or virtual machines	Each	1
	Data Storage Network (SAN) Software: This includes Fibre Channel Multipathing Software, Fabric Management and reporting function	Each	1

- All associated licenses should be included for a minimum five (5) years (centralised management console, reporting, capacity, replication, data-hold, retention, encryption, client and all other feature licenses).

- All firmware and software version upgrades should be included for a minimum five (5) years.
- All Hardware must be covered with 5-year warranty with a 6-hour fix.
- Vendor support is mandatory to maintain operational continuity and compliance with data protection regulations.
- The solution must include redundancy features, such as RAID configurations, dual power supplies, dual controllers, multiple connectivity modules.
- The hardware must be deployed with minimal downtime, requiring a phased implementation plan and comprehensive testing to ensure reliability.
- Any proposed OEMs must be fully supported by the bidder using OEM-certified staff at the equivalent requested certification levels.