TECHNICAL SPECIFICATION

Provision of a Next-Generation Wide Area Network, Secure Internet Connectivity, Managed Security, Disaster Recovery and Related Managed Services

Contract Period: 60 Months

August 2026

TECHNICAL CONTACTS

1. Principal Author: Dr. Joe Khosa

   Joek@legal-aid.co.za

2. Co-Author: Jonas Skhosana

   Jonass@legal-aid.co.za

CONTENTS

Acronyms

Acronym / Abbreviation	Meaning
3CX	3CX Cloud Telephony / IP Telephony Platform
5G	Fifth Generation Mobile Network
AIOps	Artificial Intelligence for IT Operations
APN	Access Point Name
API	Application Programming Interface
AWS	Amazon Web Services
BCP	Business Continuity Plan
CASB	Cloud Access Security Broker
CV	Curriculum Vitae
DIA	Dedicated Internet Access
DLP	Data Loss Prevention
DNS	Domain Name System
DR	Disaster Recovery
eLAA	Electronic Legal Aid Administration System
eSIM	Embedded Subscriber Identity Module
FWaaS	Firewall as a Service
GB	Gigabyte
Gbps	Gigabits per second
ICT	Information and Communications Technology
ID	Identifier
IDS	Intrusion Detection System
IDS/IPS	Intrusion Detection System / Intrusion Prevention System
IJS	Integrated Justice System
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISP	Internet Service Provider
IT	Information Technology
ITSM	Information Technology Service Management

Mbps	Megabits per second
MFA	Multi-Factor Authentication
MPLS	Multiprotocol Label Switching
NGFW	Next-Generation Firewall
NOC	Network Operations Centre
OEM	Original Equipment Manufacturer
POP	Point of Presence
QoS	Quality of Service
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SaaS	Software as a Service
SASE	Secure Access Service Edge
SD-WAN	Software-Defined Wide Area Network
SIEM	Security Information and Event Management
SIM	Subscriber Identity Module
SLA	Service Level Agreement
SSE	Security Service Edge
SWG	Secure Web Gateway
VPN	Virtual Private Network
WAN	Wide Area Network
ZTNA	Zero Trust Network Access

1. PURPOSE AND PROCUREMENT INTENT

1.1. Legal Aid South Africa requires the appointment of a suitably qualified prime service provider to design, supply, implement, migrate, manage, secure, monitor, support and continuously optimise a next-generation national Wide Area Network and associated services for a period of sixty (60) months.

1.2. The procurement is not intended to reproduce the legacy MPLS/VPN or point-to-point model on a like-for-like basis. It is intended to establish a modern digital connectivity platform that supports Legal Aid SA's current operating model and anticipated migration towards cloud-delivered services.

1.3. The service must be delivered as an integrated managed service with clear end-to-end accountability across WAN transport, Internet access, managed network security, mobility, disaster recovery connectivity and hosting, monitoring, transition and operational support.

1.4. The technical design must prioritise business and application performance. The future service must deliver fast and predictable access to eLAA and other approved internal services while simultaneously providing high-performance local or cloud-optimised access to Microsoft 365, Teams, OneDrive, Exchange Online, SaaS and general Internet services.

2. ORGANISATIONAL AND TECHNOLOGY BACKGROUND

2.1. Legal Aid South Africa is a national public entity established in terms of the Legal Aid South Africa Act 39 of 2014. Its mandate depends on reliable access to legal-administration systems, communication platforms, digital records, justice-sector integrations and secure collaboration services across a nationally distributed office footprint.

2.2. Legal Aid SA operates approximately 130 offices across all nine provinces and supports **approximately 2,600 users**. The office footprint includes National Office, Provincial Offices, Local Offices and Satellite Offices, including locations in metropolitan, urban, peri-urban and rural areas.

2.3. Legal Aid SA has progressively modernised from predominantly centralised, on-premises ICT services towards a hybrid and increasingly cloud-enabled operating model. Microsoft 365, cloud-hosted telephony, secure remote work, digital legal services and future

SaaS/cloud adoption materially change the traffic profile and design requirements of the WAN.

2.4. eLAA is Legal Aid SA's principal central business application. It is hosted at National Office and replicated to the Disaster Recovery environment. The eLAA environment comprises front-end application servers, Microsoft SQL Server database servers, Microsoft SharePoint servers and other supporting infrastructure that collectively constitute the complete eLAA application platform. The future WAN must therefore provide a protected, observable and resilient private path to eLAA while ensuring that cloud and Internet traffic does not unnecessarily consume National Office capacity.

3. CURRENT-STATE ENVIRONMENT AND BUSINESS PROBLEM

3.1. Legal Aid SA currently operates a Cisco Meraki SD-WAN environment. The current service evolved from an earlier MPLS-centric architecture and still contains traffic patterns and service dependencies that place unnecessary load on central connectivity.

3.2. The organisation's main performance challenge is not limited to raw bandwidth. The central issue is contention between business-critical internal traffic and high-volume Internet/cloud traffic, including Microsoft 365, OneDrive synchronisation, Windows and software updates, Teams, general browsing and other SaaS services.

3.3. The business requirement is therefore to achieve speed in two dimensions simultaneously: fast access to eLAA and internal services, and fast access to Internet and cloud services.

3.3.1. eLAA and approved internal services must use a protected private path to National Office or the designated hosting environment.

3.3.2. Cloud and Internet traffic must be capable of secure local or cloud-based breakout, avoiding unnecessary backhaul through National Office.

3.3.3. Operating-system updates, bulk synchronisation and similar background traffic must not be permitted to degrade eLAA, voice or collaboration traffic.

3.3.4. Branch resilience must be proportionate to site criticality and must not depend on a single carrier, route or access technology where diversity is required.

3.3.5. Security operations must be outsourced as part of the managed service because Legal Aid SA does not intend to build or maintain a large internal network-security operations capability.

3.3.6. Disaster Recovery must form part of the same service architecture and must support disk-based replication and recoverability rather than physical tape collection.

4. STRATEGIC DESIGN PRINCIPLES

Principle	Required interpretation
Application-first design	Routing, QoS, security and capacity decisions must be based on application criticality and measured path quality, not only destination network.
Internet-first/cloud-ready	Approved SaaS and Internet traffic must be able to break out locally or through cloud-delivered security controls without unnecessary backhaul.
Protected private application path	eLAA and approved internal services must remain reachable through a secure, policy-controlled private overlay or equivalent routed architecture.
Carrier and transport independence	The logical WAN must be separable from the underlying access medium and capable of using multiple carriers and technologies.
Security as a managed service	Network security must be centrally governed and operated 24x7 by the prime service provider.
Resilience by design	National Office and DR require diversity and high availability; other offices require resilience proportionate to operational criticality and feasibility.
Observable service	Legal Aid SA must be able to measure application experience, overlay, underlay, carrier, edge, security and DR performance from a common service-assurance view.
Incumbent independence	The evaluated solution must be implementable without relying on incumbent-owned equipment, licences, platforms, undocumented configurations or privileged access.
Lifecycle sustainability	All proposed equipment, software and subscriptions must remain supported throughout the five-year contract and must be refreshable where required.

Principle	Required interpretation
Recoverability, not only replication	DR must protect against operational failure and data loss. Disk-based replication must therefore be complemented by retention, versioning, immutability or equivalent recoverability controls.

Table 1: Strategic principles

5. 1. SCOPE OF SERVICES

5.1. National WAN and Software-Defined Network Services

5.1.1. The successful bidder shall provide, implement, operate, manage, monitor and support a national software-defined Wide Area Network connecting all designated Legal Aid South Africa locations for the full sixty (60) month contract period.

5.1.2. The WAN service shall support approximately 130 geographically distributed sites, comprising National Office, Provincial Offices, Local Offices, Satellite Offices, the Disaster Recovery environment and approved external or justice-sector connectivity points.

5.1.3. The proposed WAN architecture must use a centrally managed, policy-driven software-defined overlay or equivalent architecture capable of operating independently of the underlying telecommunications carrier or access technology.

5.1.4. The solution must provide, at minimum:

a) centralised orchestration and policy management;
b) encrypted site-to-site connectivity;
c) dynamic path selection;
d) application-aware routing;
e) Quality of Service;
f) network segmentation;
g) automated failover;
h) brownout detection;
i) link utilisation and performance monitoring;
j) zero-touch provisioning;
k) configuration management and rollback;
l) real-time application visibility;
m) high-availability capabilities for critical network components; and
n) IPv4 operation with IPv6 readiness.

5.1.5. The architecture must allow Legal Aid SA to change telecommunications carriers, access technologies or individual site connectivity without requiring material redesign of the logical WAN.

5.1.6. The bidder must provide a Legal Aid SA-specific architecture and may not rely solely on generic OEM diagrams or marketing material.

5.2. Primary and Secondary Internet and Access Services

5.2.1. 1The successful bidder shall provide all primary and secondary connectivity services required to deliver the contracted WAN service.

5.2.2. The initial minimum bandwidth baseline shall be:

Site category	Minimum bandwidth
National Office primary link:	**1 Gbps**
National Office Secondary link:	**1 Gbps**
Disaster Recovery site	**1 Gbps with internet breakout capabilities(scalable)**
Local Offices	**100 Mbps**
Local Offices Secondary link:	**100 Mbps**
Satellite offices	**50 Mbps**
IJS	**10Mbps**

Table 2: Option 1 bandwith requirements.

Site category	Minimum bandwidth
National Office primary link:	**1 Gbps**
National Office secondary link:	**1 Gbps**
Disaster Recovery site	**1 Gbps with internet breakout capabilities(scalable)**
Local Offices	**100Mbps**
Satellite offices	**50 Mbps**
IJS	**10Mbps**

Table 3: Option 2 bandwith requirements.

5.2.3. Bandwidth requirements constitute minimum service requirements and may be **increased or decreased** by Legal Aid SA during the contract in accordance with operational demand.

5.2.4. The service provider must provide sufficient bandwidth headroom to accommodate encryption, security inspection, SD-WAN overhead and normal growth without reducing the usable contracted service below the required capacity.

5.2.5. National Office and the Disaster Recovery environment must be provided with resilient connectivity designed to eliminate material single points of failure.

5.2.6. Secondary connectivity at critical sites must be genuinely diverse from the primary service wherever technically feasible.

5.3. Secure Local and Cloud Internet Breakout

5.3.1. The solution **must provide secure local or cloud-based Internet breakout** at Legal Aid SA offices.

5.3.2. General Internet and approved cloud traffic must not be unnecessarily backhauled through National Office.

5.3.3. Local breakout must be centrally governed and protected through the managed security architecture specified in this tender.

5.3.4. At minimum, the architecture must provide optimised access to:

a) Microsoft 365;
b) Microsoft Teams;
c) Exchange Online;
d) OneDrive;
e) approved SaaS platforms;
f) Microsoft and other approved software-update services;
g) general Internet services; and
h) future approved cloud platforms.

5.3.5. Legal Aid SA must retain the ability to define applications or destinations that may or may not use local Internet breakout.

5.3.6. The architecture must maintain consistent security controls irrespective of whether a user accesses services from National Office, a branch office, the Disaster Recovery environment or remotely.

5.4. Managed SASE/SSE Network Security Service

5.4.1. The proposed solution must incorporate a fully managed Secure Access Service Edge (SASE), Security Service Edge (SSE), or demonstrably equivalent converged cloud-delivered security architecture.

5.4.2. For purposes of this tender, a solution presented as equivalent must provide all material security outcomes specified in this section. A conventional perimeter firewall service on its own will not be regarded as equivalent.

5.4.3. The managed security service must provide, where applicable:

a) Next-Generation Firewall or Firewall-as-a-Service;
b) intrusion detection and prevention;
c) Secure Web Gateway;
d) DNS security;
e) URL and content filtering;
f) application control;
g) malware and threat prevention;
h) Zero Trust Network Access;
i) secure remote access;
j) identity-aware security policies;
k) network segmentation;
l) encrypted traffic inspection, subject to Legal Aid SA policy;
m) cloud access security capabilities;
n) Data Loss Prevention capability where required;
o) security event logging;
p) centralised security policy management;
q) threat intelligence integration;
r) supported SIEM integration; and
s) full administrative audit trails.

5.4.4. The security service must be managed on a 24x7x365 basis by the successful bidder.

5.4.5. Legal Aid SA must not be required to undertake routine firewall administration, signature management, security patching, threat-feed management or OEM escalation.

5.4.6. The bidder must clearly disclose any security functions that remain dependent on Legal Aid SA endpoint, identity, application or certificate-management services.

5.5. Zero Trust and Secure Remote Access

5.5.1. The solution must support a Zero Trust access model for users requiring access to Legal Aid SA applications from outside the corporate office environment.

5.5.2. Access decisions must, where supported, consider:

a) user identity;
b) device identity;
c) authentication status;
d) multi-factor authentication;
e) device security posture;
f) application being accessed;
g) user role;
h) source context; and
i) applicable Legal Aid SA security policy.

5.5.3. The solution must integrate with Legal Aid SA's Microsoft Entra ID or other designated identity services.

5.5.4. Remote users must not automatically receive unrestricted network-level access simply because they have authenticated.

5.5.5. Access must follow the principle of least privilege and should preferably be application-specific.

5.5.6. Remote access to eLAA must be securely authenticated, controlled, logged and auditable.

5.6. Application-Aware Routing, QoS and Dynamic Path Control

5.6.1. The proposed WAN must identify, classify, prioritise and route traffic according to business criticality and real-time network conditions.

5.6.2. eLAA must be configured as a mission-critical application class.

5.6.3. The solution must provide explicit protection for eLAA against congestion caused by:

a) Microsoft software updates;
b) operating-system updates;
c) OneDrive synchronisation;
d) bulk file transfers;
e) Internet downloads;
f) general browsing;

g) non-critical SaaS traffic; and
h) other bandwidth-intensive background applications.

5.6.4. Application-routing decisions must be capable of considering:
a) latency;
b) jitter;
c) packet loss;
d) utilisation;
e) congestion;
f) link availability; and
g) defined application policy.

5.6.5. The solution must detect a degraded or brownout condition even where the affected physical circuit remains technically operational.

5.6.6. Where thresholds are exceeded, affected traffic must automatically be moved to an alternative suitable path in accordance with approved policy.

5.6.7. The solution must provide suitable QoS for eLAA, Microsoft Teams, cloud telephony services, voice, video and other identified business-critical applications.

5.7. Multi-Carrier and Multi-Technology Underlay Management

5.7.1. The WAN must not be dependent on a single telecommunications carrier or access technology.

5.7.2. The bidder must be capable of sourcing, integrating and managing connectivity from multiple network operators.

5.7.3. Supported underlay technologies may include:
a) fibre;
b) dedicated Internet access;
c) business broadband;
d) licensed microwave;
e) fixed wireless;
f) LTE;
g) 5G;
h) satellite; and
i) other proven enterprise connectivity technologies.

5.7.4. The successful bidder remains responsible for the performance of all underlying carriers used to provide the Legal Aid SA service.

5.7.5. Legal Aid SA must not be required to separately manage or escalate faults to underlying fibre network operators, mobile operators or other carrier subcontractors.

5.8. LTE/5G and Other Resilient Access Services

5.8.1. LTE/5G or other appropriate wireless connectivity must form part of the resilience model where technically and commercially appropriate.

5.8.2. Mobile connectivity used for WAN resilience must integrate directly with the managed WAN architecture.

5.8.3. The solution must support automatic failover and restoration without requiring branch users to manually reconnect services.

5.8.4. The service must provide:

a) signal-quality monitoring;
b) data-consumption monitoring;
c) automated alerts;
d) multi-operator capability where practical;
e) external antenna options where required; and
f) centralised management.

5.8.5. LTE/5G may also be used to provide temporary connectivity to new, relocated or temporary Legal Aid SA offices while permanent connectivity is being established.

5.9. Managed Mobile-User Connectivity

5.9.1. The successful bidder shall provide a managed mobile-connectivity solution for authorised Legal Aid SA users requiring connectivity outside the corporate office environment.

5.9.2. The service must provide greater control than a conventional unrestricted mobile-data service.

5.9.3. The proposed service may incorporate managed APN, private APN, eSIM, secure Internet access, SASE-based mobile security, ZTNA or an equivalent architecture.

5.9.4. The service must provide:

a) centralised activation and suspension;
b) usage monitoring;
c) per-user and/or per-SIM thresholds;
d) pooled data options;

e) automated consumption alerts;
f) multi-network capability where appropriate;
g) application-level visibility;
h) web-category controls;
i) business-use policy enforcement; and
j) detailed consumption reporting.

5.9.5. Where technically possible, Legal Aid SA must be capable of allowing, blocking or rate-limiting specific application categories to minimise misuse and uncontrolled variable expenditure.

5.9.6. Table 4 indicates the baseline for APN requirements with two options based on data bundles per ISP choice

PN Provider	Number of Sims	Data Bundles (Option1)	Data Bundles (Option2)
MTN	500	2.5 TB	5 TB
Vodacom	500	2.5TB	5 TB

Table 4: Baseline APN Allocation

5.10. Disaster Recovery Hosting, Connectivity and Operational Support

5.10.1. Disaster Recovery services shall form an integral component of the WAN managed-service contract.

5.10.2. The successful bidder shall provide a secure and resilient DR hosting environment suitable for Legal Aid SA's designated infrastructure.

5.10.3. The DR service must include:

a) suitable rack or hosting capacity (1 Rack);
b) redundant power;
c) environmental monitoring;
d) cooling;
e) physical security;
f) controlled physical access;
g) remote-hands support;
h) resilient WAN connectivity;

i) resilient Internet connectivity;
j) managed network security;
k) replication connectivity;
l) monitoring;
m) encryption capabilities and
n) operational support.

5.10.4. The DR site must be capable of assuming designated application-connectivity and WAN roles where National Office or its connectivity becomes unavailable.

5.10.5. The bidder must describe the DR connectivity architecture, dependencies and failure domains.

5.11. Disk-Based Replication, Recovery Retention and Restore Capability

5.11.1. Legal Aid SA requires a disk-based replication and recovery solution between National Office and the Disaster Recovery environment to **replace the current tape drive offsite setup.**

5.11.2. The future service must not depend on routine **physical backup-tape collection** as the principal off-site recovery mechanism.

5.11.3. Legal Aid SA currently uses, on average, ten (10) x 10 TB backup tapes per month, equating to approximately **120 tapes per annum**. Bidders are required to propose a secure, scalable and resilient **disk-based backup and recovery solution** to replace the current tape-based arrangement.

5.11.4. Replication alone will not be considered sufficient backup protection.

5.11.5. The solution must incorporate recoverability controls capable of protecting Legal Aid SA from:

a) accidental deletion;
b) data corruption;
c) malicious deletion;
d) ransomware;
e) encryption;
f) replication of corrupted data; and
g) logical failure affecting the production environment.

5.11.6. The bidder must therefore provide appropriate:

a) versioning;
b) immutable recovery copies;

c) logically isolated recovery copies; or
d) equivalent protection mechanisms.

5.11.7. Replication health, recovery-point status, storage consumption and failures must be continuously monitored.

5.11.8. Restore capability must be periodically tested and evidenced.

5.11.9. The bidder must recommend appropriate RPO and RTO targets during detailed design for approval by Legal Aid SA.

5.11.10. The current backup software is Veam backup solution

5.12. Monitoring, Observability, Reporting and Service Assurance

5.12.1. The service must provide end-to-end monitoring beyond basic circuit availability.

5.12.2. Monitoring must include:

a) application experience;
b) *eLAA performance;
c) Internet performance;
d) overlay health;
e) underlay/carrier health;
f) latency;
g) jitter;
h) packet loss;
i) bandwidth utilisation;
j) application utilisation;
k) security status;
l) edge-device health;
m) mobile connectivity;
n) failover events;
o) DR connectivity;
p) replication health; and
q) SLA performance.

5.12.3. Legal Aid SA must receive secure access to a real-time monitoring and reporting portal.

5.12.4. The solution must provide historical reporting suitable for:

a) troubleshooting;
b) trend analysis;
c) capacity planning;

d) performance reviews;
e) SLA verification; and
f) audit purposes.

5.12.5. The bidder must provide sample dashboards and reports as part of its technical response.

5.13. 24x7 Network and Managed Security Operations

5.13.1. The successful bidder must provide 24x7x365 Network Operations Centre and managed security operations capability.

5.13.2. The service must include proactive detection, triage and management of network and security incidents.

5.13.3. Legal Aid SA users must not be the primary monitoring mechanism for detecting network failure.

5.13.4. Agreed failure and degradation conditions must automatically generate alerts and/or incidents.

5.13.5. The operating service must provide Level 1, Level 2 and Level 3/OEM escalation.

5.13.6. Major incidents must be subject to formal technical escalation, communication and root-cause analysis.

5.14. Implementation, Coexistence, Migration and Testing

5.14.1. The successful bidder shall assume full responsibility for implementation and transition of the contracted services.

5.14.2. The complete national implementation must achieve final acceptance within six **(6) months** from the agreed project commencement date.

5.14.3. A national big-bang migration will not be accepted.

5.14.4. The transition must include:

a) mobilisation;
b) discovery;
c) site surveys;
d) carrier feasibility;
e) detailed design;
f) pilot implementation;
g) coexistence;

h) migration waves;
i) testing;
j) formal site acceptance;
k) DR readiness and
l) final handover.

5.14.5. Existing services must remain available until replacement services have passed the agreed acceptance criteria.

5.14.6. Each migration must include documented rollback conditions.

5.15. Lifecycle, Licensing, Spares and Technology Refresh

5.15.1. All supplied hardware, software, cloud services and subscriptions must remain supported for the entire contract period.

5.15.2. No component may be introduced where its known lifecycle would result in unsupported production infrastructure during the contract without an approved refresh plan.

5.15.3. The successful bidder shall be responsible for:

a) licences;
b) subscriptions;
c) firmware;
d) patches;
e) security updates;
f) replacement hardware;
g) spares;
h) warranties;
i) OEM escalation; and
j) lifecycle management.

5.15.4. A formal technology review must be conducted at least annually.

5.15.5. The annual review must assess relevant developments in WAN, SASE/SSE, Zero Trust, security, 5G, satellite, cloud connectivity, automation and AIOps.

5.16. Third-Party Carrier, OEM and Subcontractor Management

5.16.1. The successful bidder shall act as the **prime service provider and single point of contractual accountability**.

5.16.2. The prime service provider remains accountable for all services delivered through:

a) telecommunications carriers;
b) fibre network operators;
c) mobile-network operators;
d) OEMs;
e) cloud providers;
f) data-centre operators;
g) subcontractors; and
h) specialist support partners.

5.16.3. Legal Aid SA must not be required to determine which underlying service provider is responsible for an incident before logging a fault.

5.16.4. Disputes between the prime contractor and its suppliers may not delay restoration of Legal Aid SA services.

5.17. Exit Management and Configuration/Data Portability

5.17.1. The service must be designed to support orderly transition to Legal Aid SA or a successor provider at the end of the contract.

5.17.2. The successful bidder must maintain current documentation throughout the contract.

5.17.3. Legal Aid SA must be capable of obtaining or exporting, in a usable format:

a) network inventory;
b) circuit inventory;
c) configurations;
d) security policies;
e) routing policies;
f) SD-WAN policies;
g) application policies;
h) asset records;
i) event data;
j) performance history;
k) service reports; and
l) relevant configuration and audit records.

5.17.4. The successful bidder must provide reasonable exit assistance, knowledge transfer and cooperation with an incoming service provider.

5.17.5. The solution must not intentionally introduce technical or contractual lock-in that prevents Legal Aid SA from changing providers at the end of the contract.

5.17.6. All Legal Aid SA configuration, operational and service-management data must remain accessible to Legal Aid SA in accordance with the contract and applicable information-governance requirements.

6. COMMON EVALUATED SOLUTION BASELINE

6.1. Every bidder must submit a complete new-solution baseline that can be implemented without reliance on incumbent-owned, customer-premises equipment, licences, management platforms, carrier contracts, proprietary configurations or privileged access.

6.2. For transition evaluation, bidders must assume a zero-incumbent-knowledge mobilisation model based on the published tender information, approved data-room information and the outgoing provider cooperation expressly required by the contract.

7. NATIONAL SITE AND BANDWIDTH BASELINE

7.1. The bidder must design for approximately 130 Legal Aid SA sites. The final site list and addresses will be issued in the site schedule and must be verified during implementation.

7.2. The following bandwidths constitute the initial minimum design baseline. Legal Aid SA reserves the right to revise individual site sizes before award or during the contract based on user numbers, application demand, utilisation and business growth.

Site category	Indicative quantity	Minimum bandwidth	Preferred access	Resilience expectation
National Office - Primary	1	1 Gbps	Dedicated enterprise-grade access	Diverse from secondary
National Office - Secondary	1	1 Gbps	Dedicated enterprise-grade access	Physically and logically diverse where feasible
Disaster Recovery	1	1 Gbps	Dedicated enterprise-grade access	Resilient replication, WAN and Internet roles
Local Offices	65	100 Mbps	Fibre preferred; equivalent enterprise access permitted	Secondary/failover required
Local Offices	65	100 Mbps	LTE or Broadband	Tiered resilience
Satellite Offices	64	50 Mbps	Fibre/fixed wireless/LTE/5G/satellite where appropriate	Cost-effective failover where required
IJS	1	10 Mbps	Secure routed connectivity or approved private service	Dedicated private link only where externally mandated

Table 5: Option 1 bandwith requirements.

Site category	Indicative quantity	Minimum bandwidth	Preferred access	Resilience expectation
National Office - Primary	1	1 Gbps	Dedicated enterprise-grade access	Diverse from secondary
National Office - Secondary	1	1 Gbps	Dedicated enterprise-grade access	Physically and logically diverse where feasible
Disaster Recovery	1	1 Gbps	Dedicated enterprise-grade access	Resilient replication, WAN and Internet roles
Local Offices	65	100 Mbps	Fibre preferred; equivalent enterprise access permitted	Tiered resilience
Satellite Offices	64	50 Mbps	Fibre/fixed wireless/LTE/5G/satellite where appropriate	Cost-effective failover where required
IJS	1	10 Mbps	Secure routed connectivity or approved private service	Dedicated private link only where externally mandated

Table 6: Option 2 bandwith requirements.

7.3. All bandwidth must be provisioned with sufficient headroom for encryption, security inspection, overlay overhead and anticipated growth. The bidder must state any licensing or throughput constraint that reduces usable performance when all proposed security and SD-WAN features are enabled.

7.4. The managed service must include capacity management and published upgrade triggers based on sustained utilisation, congestion, application experience and growth.

8. TARGET WAN ARCHITECTURE

8.1. The bidder must provide a Legal Aid SA-specific target architecture showing all site tiers, National Office, DR, local/cloud Internet breakout, private eLAA paths, managed security enforcement, mobility and partner connectivity.

8.2. The solution must support an enterprise-grade software-defined WAN or equivalent policy-driven architecture with:

8.2.1. centralised orchestration and policy management

8.2.2. transport-independent encrypted overlay

8.2.3. dynamic path selection

8.2.4. application-aware routing

8.2.5. brownout detection

8.2.6. automatic failover and controlled restoration

8.2.7. load balancing where appropriate

8.2.8. network segmentation

8.2.9. zero-touch provisioning

8.2.10. configuration versioning and rollback

8.2.11. high-availability control/management components where required

8.2.12. IPv4 operation with IPv6 readiness

8.3. Routing and traffic forwarding must continue according to established policy if the central management or orchestration platform becomes temporarily unavailable.

8.4. The architecture must not create a new single point of failure at National Office, DR, the security service edge or the orchestration layer.

9. APPLICATION-AWARE ROUTING AND eLAA PERFORMANCE PROTECTION

9.1. eLAA must be treated as a mission-critical application class.

9.2. The solution must identify eLAA traffic and apply explicit QoS and path policy to protect it from congestion caused by Internet, cloud synchronisation, software updates, bulk downloads and other lower-priority traffic.

9.3. The solution must support traffic shaping, scheduling, rate limiting, deprioritisation and/or application steering for operating-system updates, software distribution, synchronisation and bulk traffic.

9.4. The bidder must demonstrate the ability to measure the complete service path affecting eLAA, including branch edge, overlay, underlay/carrier, National Office edge and relevant internal handoff.

9.5. The solution must make path decisions using measurable conditions including latency, jitter, packet loss, utilisation and path availability.

9.6. The service must detect degradation while a link remains technically up and must be able to move affected applications to a healthier path according to policy.

9.7. The solution must preserve voice and real-time traffic during congestion and must support Microsoft Teams and 3CX with suitable QoS.

10. INTERNET, CLOUD AND MICROSOFT 365 OPTIMISATION

10.1. Legal Aid SA requires secure local or cloud-based Internet breakout at branch offices. Internet traffic must not be backhauled through National Office unless explicitly required by policy.

10.2. The design must optimise access to Microsoft 365, Teams, Exchange Online, OneDrive, approved SaaS applications and future cloud services.

10.3. The bidder must describe any Microsoft peering, cloud on-ramp, SaaS optimisation or equivalent routing capabilities included in the service.

10.4. The architecture must support future Azure, AWS or other approved cloud connectivity without requiring wholesale WAN redesign.

10.5. Secure breakout must remain subject to centrally governed policy and consistent logging irrespective of user or site location.

11. UNDERLAY, CARRIER DIVERSITY AND RESILIENCE

11.1. The solution must support multiple underlay technologies, including fibre, dedicated Internet access, business broadband, licensed microwave, fixed wireless, LTE/5G, satellite and other proven enterprise access methods.

11.2. National Office and DR must have diverse connectivity, high-availability edge capability and automatic failover.

11.3. Bidders must provide a documented method for verifying failure-domain diversity, including:

11.3.1. last-mile owner

11.3.2. physical route and ducting

11.3.3. building entry

11.3.4. exchange/POP

11.3.5. upstream carrier

11.3.6. shared infrastructure or reseller dependencies

11.3.7. power dependencies where relevant

11.3.8. common risk groups

11.4. Two services sold by different resellers will not be treated as diverse where they share the same material failure domain.

11.5. Branch resilience must be proportionate to site criticality, geography and feasibility. Rural or hard-to-reach sites may use fixed wireless, LTE/5G or satellite where this provides a more reliable outcome than fibre.

11.6. The service must support temporary connectivity for new or relocating offices when permanent circuits are delayed.

12. MANAGED SECURITY, SASE/SSE AND ZERO TRUST

12.1. Network security must be provided as a fully managed 24x7 service. Legal Aid SA does not intend to depend on a large internal security operations capability for day-to-day administration of the WAN security stack.

12.2. The bidder must provide SASE, SSE or an equivalent modern secure-network architecture that integrates or interoperates with the proposed WAN.

Control domain	Minimum service expectation
Network firewalling	Managed NGFW/FWaaS, segmentation and policy enforcement
Threat prevention	IDS/IPS, malware protection, DNS security and threat intelligence
Web security	Secure Web Gateway, URL/category filtering and application control
Zero Trust	User/device identity, MFA integration, posture where supported, least privilege and application-based access
Cloud controls	CASB and DLP capability where required and technically appropriate
Identity	Integration with Microsoft Entra ID or equivalent Legal Aid SA identity services
Encryption	Strong encrypted overlays and secure remote access
Operations	24x7 monitoring, triage, incident coordination, patching, threat feeds and OEM escalation
Auditability	Exportable logs, approved policy changes, administrator audit trail and retention
SIEM/API	Supported log export and integration through standard interfaces

Table 7: Security requirements

12.3. Bidders must explicitly disclose limitations and shared responsibilities relating to encrypted-traffic inspection, certificate management, endpoint controls, identity dependencies, privacy and application-owner responsibilities.

12.4. Security policy must follow the user/device and application context where supported, not only the physical branch.

13. MOBILITY AND REMOTE-USER CONNECTIVITY

13.1. The future mobile service must move beyond a purely consumption-based APN model. It must provide centrally managed, policy-controlled mobile connectivity for authorised users and devices.

13.2. The bidder may propose private APN, managed APN, eSIM, SASE mobile access, ZTNA or an equivalent secure architecture.

13.2.1. multi-operator support where practical

13.2.2. pooled data and per-user/SIM controls

13.2.3. usage thresholds and automated alerts

13.2.4. central activation, suspension and reporting

13.2.5. application and web-category controls

13.2.6. ability to restrict or rate-limit non-business traffic where technically possible

13.2.7. secure access to eLAA and approved internal services

13.2.8. integration with the common security policy framework

13.3. Remote users on private Wi-Fi or public Internet must be capable of secure access without requiring all traffic to traverse National Office. Zero Trust or equivalent identity-aware access should be used for private applications where appropriate.

14. DISASTER RECOVERY, DISK-BASED REPLICATION AND RECOVERABILITY

14.1. Disaster Recovery hosting and connectivity form part of this procurement and must be delivered under the prime service provider's end-to-end accountability.

14.2. Legal Aid SA's production environment is hosted at National Office and replicated to the DR environment. The new service must provide resilient replication, WAN, security and Internet connectivity to DR.

14.3. The future service will not use physical tape collection as the primary off-site recovery mechanism. The bidder must provide a disk-based replication and recovery architecture.

14.4. Replication alone will not be accepted as equivalent to backup. The proposed architecture must provide recoverability controls such as retention, versioning, immutable recovery copies, logically isolated recovery copies or equivalent mechanisms that protect against deletion, corruption and malicious encryption.

Area	Requirement
Facility	Resilient power, cooling, physical security, environmental monitoring, controlled access and remote support
Connectivity	1 Gbps baseline, resilient WAN and Internet connectivity, suitable replication paths and alternate application-connectivity role.
Hosting	Sufficient rack/cabinet capacity and associated data-centre services for Legal Aid SA DR equipment or approved hosted recovery infrastructure
Replication	Monitored disk-based replication with bandwidth protection and failure alerting
Recovery copies	Retention/versioning/immutability or equivalent recoverability control
Testing	Planned and evidenced failover, restore and failback testing
Operational reporting	Replication health, capacity, recovery-point status, incidents and test results
Growth	Scalable storage and bandwidth without disruptive redesign
Internet breakout	The DR must have internet breakout capabilities.

Table 8: DR requirements.

14.5. The bidder must propose measurable Recovery Point Objective (RPO) and Recovery Time Objective (RTO) commitments for the DR services after completing technical discovery. Final values will be agreed during detailed design and incorporated into the SLA.

14.6. DR must be capable of assuming approved application-connectivity roles when National Office connectivity is unavailable, subject to Legal Aid SA's application and infrastructure design.

14.7. Recovery testing must include National Office path loss, carrier failure, Internet failure, security-service failure, DR routing, application connectivity, restore verification and controlled restoration.

15. MONITORING, OBSERVABILITY AND SERVICE ASSURANCE

15.1. Monitoring must provide end-to-end service visibility and may not be limited to link up/down status.

15.1.1. user/application experience
15.1.2. eLAA path performance
15.1.3. SD-WAN overlay
15.1.4. underlay/carrier performance
15.1.5. edge-device health
15.1.6. security service status
15.1.7. DR connectivity and replication health
15.1.8. latency, jitter and packet loss
15.1.9. bandwidth and application utilisation
15.1.10. failover/brownout events
15.1.11. configuration changes
15.1.12. incident status and SLA measurement

15.2. Legal Aid SA must receive secure portal access to real-time and historical service data.

15.3. Agreed failures and degradation conditions must automatically generate incidents or alerts without waiting for end-user reporting.

15.4. The service should provide event correlation, anomaly detection, capacity forecasting and root-cause assistance. Bidders must distinguish production capability from roadmap capability.

15.5. Data must be exportable, and documented API/webhook or ITSM integration must be available for supported service events.

15.6. Historical performance data must be retained for at least twelve (12) months, unless the bidder proposes a longer period at no material cost.

16. MANAGED SERVICE MODEL AND GOVERNANCE

16.1. The bidder must operate a 24x7x365 managed service covering all contracted WAN, Internet, security, DR and associated services.

16.2. The prime service provider remains responsible for all included carriers, OEMs, subcontractors, hosting providers and support organisations.

16.3. The operating model must include incident, major incident, problem, change, configuration, capacity, availability, security and service-level management.

16.4. The service governance model must include:

16.4.1. named Service Manager

16.4.2. Technical Account Manager or equivalent

16.4.3. executive escalation contact

16.4.4. monthly operational service review

16.4.5. quarterly strategic service review

16.4.6. annual technology and architecture review

16.4.7. continual-service-improvement register

16.4.8. risk and action register

17. SERVICE-LEVEL REQUIREMENTS

Service class	Typical scope	Acknowledgement/response	Restore target	Availability
Critical	National Office, DR, critical integration services	30 minutes	2 hours	99.95% or better
High	Provincial and Local Offices	30 minutes	4 hours	99.50% or better
Standard	Other Local and Satellite Offices	60 minutes	8 hours	99.00% or better

Table 9: SLA requirements.

17.1. Bidders must submit a binding SLA with calculation rules for availability, acknowledgement, restoration, failover, reporting, security notification and service credits/penalties.

17.2. The SLA must define maintenance windows, exclusions, chronic degradation, repeat-failure treatment and service-credit mechanisms.

17.3. The service must monitor and report latency, packet loss and jitter as contractual performance indicators. The following baseline should be used unless the bidder proposes demonstrably better values:

Path class	Latency	Packet loss	Jitter
National Office / DR fibre path	< 20 ms where technically feasible	< 1%	< 20 ms
National branch fibre/fixed path	< 50 ms within South Africa	< 1%	< 30 ms
Wireless/LTE/5G/satellite	Technology-appropriate thresholds to be declared	< 1% target where feasible	Technology-appropriate

Table 10: Peformance requirements.

17.4. SLA measurement must be based on service evidence available to both parties and must support independent verification by Legal Aid SA.

18. IMPLEMENTATION, MIGRATION AND TRANSITION

18.1. The complete solution must be implemented, stabilised and finally accepted within six (6) months from the agreed project commencement date.

18.2. A national big-bang cutover will not be accepted.

18.2.1. mobilisation and common-baseline confirmation

18.2.2. site discovery and surveys

18.2.3. carrier feasibility and diversity validation

18.2.4. high-level and low-level design

18.2.5. pilot implementation

18.2.6. controlled migration waves

18.2.7. coexistence with incumbent services

18.2.8. site acceptance testing

18.2.9. DR readiness and recovery testing

18.2.10. hypercare/stabilisation

18.2.11. final operational handover

18.3. The incumbent and new environments must coexist safely until the replacement service at each site has passed acceptance testing.

18.4. No existing circuit should be terminated until the replacement service has been formally accepted and the agreed rollback window has expired.

18.5. Each cutover plan must define change control, success criteria, rollback triggers and evidence for eLAA, Internet, voice, security and failover testing.

19. EQUIPMENT, LICENSING, LIFECYCLE AND EXIT MANAGEMENT

19.1. All proposed products, subscriptions and services must remain vendor-supported throughout the sixty-month contract, including required updates and upgrades.

19.2. The bidder must supply all licences necessary to deliver the specified features at the proposed throughput. Feature enablement may not materially reduce performance below the contracted design.

19.3. The bidder must provide spares, field replacement and lifecycle management for supplied equipment.

19.4. An annual technology review must assess SD-WAN, SASE/SSE, Zero Trust, 5G, satellite, cloud connectivity, AIOps and relevant security developments.

19.5. The service must avoid unnecessary lock-in. Legal Aid SA must be able to export representative configuration, policy, inventory, event and reporting data.

19.6. Exit obligations must include a current asset/service inventory, configuration and policy export, documentation, transition support and reasonable cooperation with a successor provider.

20. PROJECT GOVERNANCE DELIVERABLES

20.1. The following governance documents must be delivered as part of the submission:

20.1.1. Project Charter and governance structure

20.1.2. Detailed integrated project schedule

20.1.3. Work Breakdown Structure

20.1.4. Resource plan and responsibility matrix

20.1.5. Risk and issue management plan

20.1.6. Site survey and readiness reports

20.1.7. Carrier feasibility and diversity evidence

20.1.8. High-Level Design

20.1.9. Low-Level Design

20.1.10. Security architecture and policy matrix

20.1.11. Migration and coexistence plan

20.1.12. Cutover runbooks and rollback plans

20.1.13. Testing and acceptance plan

20.1.14. DR architecture and recovery test plan

20.1.15. Communications and change-management plan

20.1.16. Configuration and asset inventory

20.1.17. Training and knowledge-transfer plan

20.1.18. Operational handover pack

20.1.19. As-built documentation

20.1.20. Service stabilisation and final acceptance report

21. BIDDER TECHNICAL RESPONSE REQUIREMENTS

21.1. The bidder must provide a structured technical response cross-referenced to this specification and the evaluation criteria.

Ref	Required technical returnable	COMPLY/NOT COMPLY	BID Reference (page number)
R1	Executive summary and solution overview		
R2	Legal Aid SA-specific target architecture and traffic-flow diagrams		
R3	Bill of materials, subscriptions and dependency schedule		
R4	Underlay, carrier and diversity design		
R5	Application-performance design, including eLAA and Microsoft 365		
R6	Managed security operating model and responsibility matrix		
R7	Monitoring, observability and service-assurance model with sample dashboards/reports		
R8	DR facility response, disk-replication and recoverability design		
R9	Six-month integrated implementation and transition plan		
R10	Draft binding SLA and service-credit/penalty model		
R11	Lifecycle confirmation and authority-to-supply/support evidence		
R12	Relevant company experience, references and proposed project team		
R13	Compliance, commitment and deviation schedules		

Table 11: Technical requirements.

22. MANDATORY TECHNICAL REQUIREMENTS

The following requirements are material prerequisites. Failure to satisfy any one requirement, or to provide the required supporting evidence, will render the bid technically non-responsive.

BIDDERS MUST CROSS REFERENCE THE MANDATORY ID AS PART OF THEIR BID RESPONSE.

ID	Mandatory requirement	Minimum condition	Required evidence	COMPLY/NOT COMPLY
MR-01	Complete integrated service	Proposal covers WAN, Internet, managed security, mobility, DR, monitoring, transition and 60-month operations.	Scope cross-reference and architecture	
MR-02	Complete new-solution baseline	Solution can be implemented without reliance on incumbent-owned equipment, licences, platforms, configurations or contracts.	Signed confirmation, bill of materials and dependency schedule	
MR-03	Prime accountability	Bidder accepts end-to-end accountability for included carriers, OEMs, subcontractors, hosting and support.	Responsibility matrix and signed commitment	
MR-04	Secure application-aware architecture	Design supports secure local/cloud Internet breakout and a protected private path for eLAA and approved internal services.	Legal Aid SA-specific traffic-flow diagrams	
MR-05	Managed security	Bidder provides 24x7 managed network-security operations with incident handling and centrally governed policy.	Security operating model	

ID	Mandatory requirement	Minimum condition	Required evidence	COMPLY/NOT COMPLY
MR-06	Resilient National Office and DR	Solution provides diverse connectivity, high-availability edge capability and automated failover for National Office and DR.	Architecture and diversity method	
MR-07	DR service	Proposal includes complete DR hosting, connectivity, disk-based replication/recovery, operational support and testing scope.	Facility and service response	
MR-08	Implementation period	Bidder presents a credible plan for implementation and final acceptance within six months.	Integrated project schedule and resource plan	
MR-09	Lifecycle support	All proposed products, subscriptions and services will remain supported for the five-year contract, including required upgrades.	OEM/platform lifecycle confirmation	
MR-10	Technical response completeness	Bidder completes all compliance, commitment, deviation, bill-of-materials and evidence schedules.	Completed tender returnables	
MR-11	Authority to supply and support	Bidder or disclosed delivery partner is authorised and competent to supply and support each proposed platform.	OEM/technology support letters or equivalent evidence	
MR-12	No technical pricing contamination	Technical submission contains no pricing information where a two-envelope process applies.	Submission verification	

23. WRITTEN TECHNICAL FUNCTIONALITY EVALUATION - 80 POINTS

BIDDERS MUST CROSS REFERENCE THE CRITERION SECTION AS PART OF THEIR BID RESPONSE.

Ref	Functional area	Points
A	Legal Aid SA-specific architecture and application performance	15
B	Underlay, resilience and verified failure-domain diversity	10
C	Managed security, SASE/SSE and Zero Trust	11
D	Monitoring, application experience and service assurance	7
E	DR hosting, continuity and recovery readiness	7
F	Transition, migration and incumbent independence	13
G	Managed-service model, SLA and governance	8
H	Comparable delivery evidence and key personnel	9
	TOTAL	80

24. SCORING METHODOLOGY

A bidder must satisfy every mandatory technical requirement and achieve at least 78 points out of 80 across the written functionality.

23.1 Criterion A

Sub-Criteria	Assessment	Points [15]	Evidence Standard	Points Allocation
A1	**Target Architecture, Application Performance, Cloud Optimisation and Scalability**	**15**	The bidder must provide a complete Legal Aid SA-specific target architecture demonstrating how the proposed solution will support all site tiers, National Office, Disaster Recovery, secure local/cloud Internet breakout, protected private eLAA connectivity, Microsoft 365 and SaaS access, Teams/3CX voice and collaboration, application-aware QoS and routing, update/bulk-traffic controls, capacity management and future scalability. The design must clearly identify technical dependencies and material failure domains.	
			Compliant: The bidder provides a complete Legal Aid SA-specific architecture covering all site tiers, National Office, DR, secure local/cloud Internet breakout, protected private eLAA paths, managed security enforcement, mobility and approved partner connectivity; demonstrates explicit identification and prioritisation of eLAA using QoS and dynamic path policies; protects eLAA, Teams and 3CX from congestion and degraded paths; optimises Microsoft 365, OneDrive, Exchange Online and SaaS/cloud access; provides clear controls for shaping, scheduling, rate-limiting or deprioritising Windows/software updates, synchronisation and bulk traffic; and provides a documented capacity-sizing and scalability methodology based on user numbers, application demand, concurrency, measured utilisation, performance headroom, growth projections and defined bandwidth-upgrade triggers. Dependencies and material failure domains are clearly identified.	**15**
			Non-compliant: Any material element of the required target architecture, eLAA performance protection, Microsoft 365/cloud optimisation, Teams/3CX QoS, application-aware routing, update/bulk-traffic management, capacity-sizing methodology,	**0**

			scalability or identification of dependencies/failure domains is omitted, only partially addressed, unsupported by adequate evidence, or the bidder submits a generic architecture that is not specifically designed for the Legal Aid SA environment.	

23.2 Criterion B - Multi-Carrier and Multi-Technolog

Sub-Criteria	Assessment	Points [10]	Evidence Standard	Points Allocation
B1	**Multi-Carrier, Multi-Technology Underlay, Verified Diversity and Site Resilience**	**10**	The bidder must demonstrate a complete resilient underlay and access design that uses appropriate combinations of fibre, broadband, microwave, fixed wireless, LTE/5G, satellite or other suitable enterprise technologies. The design must avoid dependency on a single carrier or failure domain, provide a documented method for verifying genuine last-mile diversity, detect both outages and brownout conditions, support automated failover and controlled restoration, and apply resilience proportionately across National Office, DR, Provincial, Local, Satellite and rural/remote sites.	
			Compliant: The bidder provides a complete multi-carrier and multi-technology resilience design; clearly identifies primary and secondary access methods by site tier; demonstrates a documented method for verifying last-mile owner, physical route, ducting, building entry, POP/exchange, upstream carrier, power and shared-risk dependencies; provides automated failover and brownout detection based on latency, jitter, packet loss, utilisation and link health; demonstrates controlled restoration to the preferred path; and provides a resilience model proportionate to National Office, DR, Provincial, Local, Satellite and hard-to-reach locations, supported by realistic feasibility assumptions.	**10**
			Non-compliant: Any material element of the required multi-carrier design, access-technology diversity, failure-domain verification, brownout detection, automated failover, controlled restoration or site-tier resilience is omitted, only partially addressed, unsupported by adequate evidence, or the design relies	**0**

			materially on a single carrier, shared failure domain or unsupported feasibility assumption.	

23.3 Criterion C - Managed Security Architecture

Sub-Criteria	Assessment	Points [11]	Evidence Standard	Points Allocation
C1	**Managed Security Architecture, SASE/SSE and Zero Trust Capability**	**11**	The bidder must demonstrate a complete, integrated and fully managed security architecture for the proposed WAN environment. The solution must provide SASE, SSE or demonstrably equivalent converged security capabilities and must address firewalling, intrusion prevention/detection, secure web and DNS security, malware and threat prevention, URL/application control, segmentation, Zero Trust access, identity integration, logging, SIEM integration, auditability, 24x7 managed security operations and clear disclosure of shared responsibilities and technical limitations.	
			Compliant: The bidder provides a complete managed security solution addressing all required capabilities, including managed NGFW/FWaaS, IDS/IPS, Secure Web Gateway, DNS security, malware/threat prevention, URL and application control, network segmentation, Zero Trust Network Access, user/device identity, MFA integration, least-privilege access, Microsoft Entra ID or equivalent integration, 24x7 security monitoring and triage, incident coordination, patching, threat feeds, OEM escalation, exportable and retained security logs, supported SIEM integration, administrator audit trails, approved policy-change controls, and explicit disclosure of inspection, privacy, certificate, endpoint, identity and application-owner dependencies.	**11**
			Non-compliant: Any material security capability, managed-security operational requirement, identity/Zero Trust requirement, logging/SIEM requirement, auditability requirement or shared-responsibility disclosure is omitted, only partially	**0**

			addressed, unsupported by sufficient evidence, or the bidder proposes only a conventional perimeter firewall service without the required integrated SASE/SSE or equivalent capabilities.	

23.4 Criterion D - End-to-End Monitoring

Sub-Criteria	Assessment	Points [7]	Evidence Standard	Points Allocation
D1	**End-to-End Monitoring, Proactive Incident Management and Service Assurance**	7	The bidder must demonstrate a complete monitoring and service-assurance capability covering user/application experience, WAN overlay, underlay/carrier performance, SD-WAN edge devices, managed security services, Disaster Recovery components and relevant application paths. The solution must provide proactive incident detection, event correlation, root-cause analysis, SLA reporting, secure portal access and exportable data or integration capability.	
			Compliant: The bidder provides a complete end-to-end monitoring and service-assurance solution that covers application experience, overlay, underlay, carrier, edge, security and DR components; automatically detects agreed failures and degradation conditions; generates incidents or alerts proactively; provides event correlation and root-cause analysis; provides dashboards and reports that correlate application, network and infrastructure conditions; supports SLA measurement and reporting; provides secure portal access to Legal Aid SA; and supports exportable data together with documented API, webhook or ITSM integration capability.	7
			Non-compliant: Any material element of the required monitoring, proactive incident management, root-cause analysis, SLA reporting, portal access, data export or integration capability is omitted, only partially addressed, unsupported by adequate evidence, or the proposed solution does not provide complete end-to-end service assurance.	**0**

23.5 Criterion E – Disaster Recovery

Sub-Criteria	Assessment	Points [7]	Evidence Standard	Points Allocation
E1	**Disaster Recovery Hosting, Connectivity, Recoverability and Operational Readiness**	7	The bidder must demonstrate a complete Disaster Recovery service covering resilient facility infrastructure, hosting capability, WAN and Internet connectivity, disk-based replication, recovery retention, recoverability controls, failover and failback, restore testing, operational procedures, escalation and reporting. The DR solution must support recovery from infrastructure failure, connectivity failure, accidental deletion, corruption and cyber-related incidents.	
			Compliant: The bidder provides a complete DR solution addressing all required facility, hosting, connectivity, replication, recoverability, testing and operational-support requirements. The response must include evidence of resilient power and cooling, physical and environmental controls, required hosting/rack capacity, resilient WAN and Internet connectivity, disk-based replication, retention/versioning/immutability or equivalent recovery controls, failover/failback procedures, restore testing, monitoring, escalation and reporting.	7
			Non-compliant: Any material element of the required DR service is omitted, only partially addressed, unsupported by adequate evidence, or the proposed solution does not meet the specified DR and recoverability requirements.	**0**

23.6 Criterion F – Implementation Plan (11 points)

Sub-Criteria	Assessment	Points [13]	Evidence Standard	Points Allocation
F1	**Mobilisation, Discovery and Incumbent Independence**	**3**	The bidder must demonstrate a structured mobilisation and discovery approach that can commence from the common information baseline provided in the tender without reliance on undocumented incumbent knowledge, proprietary configurations, incumbent-owned tools or privileged access. The response must address site surveys, information gaps, assumptions, risks, third-party coordination, access governance and controlled change approval.	
			Compliant: The bidder provides a complete mobilisation and discovery approach based on zero-incumbent knowledge, with detailed discovery activities, site surveys, information-gap management, assumptions, risk controls, third-party coordination, access governance and clear measures to avoid dependency on incumbent proprietary assets, configurations or knowledge.	3
			Non-compliant: Any material element of mobilisation, discovery, information-gap management, third-party coordination, access governance or incumbent-independence is omitted, only partially addressed, unsupported by adequate evidence, or the approach materially depends on the incumbent's proprietary knowledge, tools, configurations or access.	**0**
F2	**Migration, Cutover, Rollback and Six-Month Implementation**	**10**	The bidder must provide a complete phased migration and implementation plan demonstrating how the current and new environments will safely coexist through pilot and migration waves, how cutovers will be controlled, how rollback will be executed, how eLAA, Internet, voice, security and failover will be tested, and how the entire implementation will achieve final acceptance within six (6) months.	
			Compliant: The bidder provides a detailed and credible six-month integrated implementation plan covering coexistence, pilot deployment, migration waves, critical path, carrier lead times, resource allocation, DR readiness, change control, cutover sequencing, acceptance criteria, eLAA/Internet/voice/security/failover testing, rollback triggers, restoration procedures, hypercare and final operational acceptance.	**10**
			Non-compliant: Any material element of coexistence, migration sequencing, cutover control, rollback, acceptance testing, carrier dependency management, resource planning, DR readiness, hypercare or the six-month completion requirement is omitted, only partially addressed, unsupported by adequate evidence, or the proposed plan cannot credibly achieve final acceptance within six months.	**0**

23.7 Criterion G - Managed service, SLA and governance (7 points)

Sub-Criteria	Assessment	Points [8]	Evidence Standard	Points Allocation
G1	**Prime Service Ownership**	**2**	The bidder must accept full end-to-end accountability for all contracted services, including telecommunications carriers, OEMs, hosting providers, managed security services, subcontractors and other third parties. The bidder must provide a clear responsibility matrix and escalation model confirming that Legal Aid SA will have a single point of contractual accountability for incident ownership, service restoration and escalation.	
			Compliant: The bidder fully accepts end-to-end accountability, provides a comprehensive responsibility matrix and escalation model, and confirms that Legal Aid SA will not be required to manage or escalate directly with underlying carriers, OEMs, hosting providers or subcontractors.	**2**
			Non-compliant: Any material element of end-to-end accountability, responsibility allocation or escalation ownership is omitted, inadequately addressed, or transferred to Legal Aid SA or another third party.	**0**
G2	**Operational Processes**	**3**	The bidder must demonstrate a comprehensive and integrated managed-service operating model covering incident management, major incident management, problem management, change management, configuration management, capacity management, availability management, security management, service continuity and continual service improvement. The response must clearly define roles, workflows, escalation paths, governance interfaces and reporting outputs.	
			Compliant: All required service-management processes are fully addressed and demonstrated as an integrated operating model, with clear roles, workflows, escalation paths, governance interfaces and measurable reporting outputs.	**3**
			Non-compliant: Any material service-management process is omitted, inadequately addressed, not integrated into the operating model, or supported only by generic statements without sufficient evidence.	**0**
G3	**Binding Punitive Service Level Agreement**	**3**	The bidder must submit a proposed binding SLA containing measurable and contractually enforceable commitments covering service availability, incident acknowledgement and response, restoration, failover, latency, jitter, packet loss, reporting, security-event notification, escalation, chronic service degradation and service credits or penalties. The SLA must include clear measurement and calculation rules.	
			Compliant: The submitted SLA fully addresses all required service measures and includes clear, measurable and enforceable calculation rules for availability, restoration, performance, failover, security notification, escalation and service credits or penalties.	**3**
			Non-compliant: Any material SLA requirement is omitted, inadequately defined, not measurable, not contractually enforceable, or the submitted SLA does not include clear calculation rules aligned to the SLA table 10.	**0**

23.8 Criterion H - Reference and key personnel (9 point)

Sub-Criteria	Assessment	Points [9]	Evidence Standard / Points Allocation Criteria	Points Allocation
H1	**Relevant Written References**	**3**	The bidder must provide written reference letters for successfully completed or currently operational projects of similar nature, scale and complexity. Relevant projects must demonstrate experience in integrated managed WAN/SD-WAN, managed security and/or Disaster Recovery services. Each reference must be **dated**, **signed** on the client's official letterhead and contain verifiable contact details. Legal Aid SA reserves the right to verify all references.	
			Five (5) or more positive and verifiable reference letters for projects of similar nature, scale and complexity.	**3**
			Three (3) to four (4) positive and verifiable reference letters for projects of similar nature, scale and complexity.	**2**
			One (1) to two (2) positive and verifiable reference letters for projects of similar nature, scale and complexity.	**1**
			No qualifying reference letters, references cannot be verified, or submitted references are not relevant to the required services.	**0**
H2	**Quality and Completeness of the Technical Project Team**	**3**	The bidder must provide a complete **named** technical team consisting, at minimum, of the following four (4) resources: **Senior Solution Architect, Senior Security Engineer, Senior Network Engineer, and Senior Systems Engineer responsible for backup, replication and Disaster Recovery services.** Each resource must have relevant qualifications and/or current professional or OEM certification applicable to the role, together with demonstrable experience relevant (5 years and above) to the proposed solution. CVs and supporting qualification/certification evidence must be submitted.	
			Compliant: All four (4) required named technical resources are provided, namely Senior Solution, Senior Architect, Senior Security Engineer, Senior Network Engineer and Senior Systems Engineer for backup/DR, and each resource is supported by a relevant CV and appropriate qualification and/or current professional/OEM certification demonstrating competence for the assigned role.	**3**
			Non-compliant: Any one of the four required technical resources is not provided, is not specifically assigned to the Legal Aid SA project, or does not have adequate supporting CV, qualification, certification or evidence of relevant competence.	**0**
H3	**Senior Project Manager**	**3**	The bidder must provide a dedicated named Senior Project Manager responsible for the implementation and transition of the Legal Aid SA solution. The Project Manager must have a minimum of **ten (10) years'**	

			relevant project-management experience and must hold a recognised project-management qualification, degree or professional certification relevant to the role, for example PMP, PRINCE2, postgraduate project-management qualification or equivalent. A detailed CV and supporting qualification/certification evidence must be submitted.	
			Compliant: A dedicated Project Manager is named, has at least ten (10) years' relevant project-management experience and holds an appropriate recognised project-management degree, qualification or professional certification. Supporting CV and documentary evidence are provided.	**3**
			Non-compliant: The Project Manager has less than ten (10) years' relevant experience, does not hold an appropriate project-management degree/qualification/certification, is not clearly assigned to the Legal Aid SA project, or the required supporting evidence is not submitted.	**0**

25. SCRIPTED TECHNICAL VERIFICATION (PRESENTATION) - 20 POINTS

Only bidders meeting the prescribed written-evaluation requirement will be invited to technical verification. Legal Aid SA will issue one script, dataset, scenario description and time allocation to all invited bidders. Demonstration may use an OEM laboratory, bidder laboratory or controlled environment.

ID	Scenario	Points [20]	Required Demonstration / Points Allocation
V1	**Application Performance Protection, Brownout Detection and Dynamic Path Selection**	**6**	The bidder must demonstrate protection of business-critical traffic under congestion and degraded-link conditions. The demonstration must generate bulk/update traffic using at least **80% of simulated branch capacity**, identify and classify eLAA as a critical application, apply the required QoS/priority policy, and show application-performance telemetry. While keeping the primary path technically operational, the bidder must introduce increased latency, jitter and/or packet loss and demonstrate brownout detection, automatic movement of affected application traffic to a healthier path, event recording and controlled restoration to the preferred path once service conditions normalise. **Compliant: 6 points. Non-compliant or incomplete demonstration: 0 points.**
V2	**Secure Internet Breakout, Identity-Aware Access and Security Enforcement**	**5**	The bidder must demonstrate secure local/cloud Internet breakout and identity-aware security controls. The demonstration must show differentiated policy outcomes for authorised users and devices, cloud/SaaS traffic, private eLAA access and blocked or restricted

			traffic. The bidder must also trigger an agreed security test event and demonstrate detection, policy enforcement, event context, security logging, log export, triage, escalation and notification workflow. **Compliant: 5 points. Non-compliant or incomplete demonstration: 0 points.**
V3	**End-to-End Monitoring, Fault Isolation, Automated Incident Management and Auditability**	**5**	The bidder must demonstrate end-to-end service visibility across the application, SD-WAN overlay, carrier/underlay, edge device and managed-security environment. The demonstration must show correlation of an application symptom with the underlying technical condition, identification of the probable fault domain/root cause and automatic creation of an incident containing relevant diagnostic evidence. The bidder must further demonstrate export of representative configuration, policy, inventory, event and reporting data together with administrator activity and configuration-change audit history. **Compliant: 5 points. Non-compliant or incomplete demonstration: 0 points.**
V4	**Disaster Recovery Connectivity, Failover and Service Continuity**	**4**	The bidder must demonstrate or appropriately simulate loss of the National Office connectivity path and the controlled establishment of the approved Disaster Recovery connectivity path. The demonstration must show WAN/routing failover, continued access to the designated service or simulated application, security-policy continuity, event/alert generation and controlled restoration or failback to the preferred production path. **Compliant: 4 points. Non-compliant or incomplete demonstration: 0 points.**

BIDDER MUST SCORE 16 POINTS TRANSLATED TO 80% ON TECHNICAL VERIFICATION STAGES IN ORDER TO PROCEED TO PRICE AND SPECIFIC-GOALS EVALUATION

26. PRICING AND PREFERENTIAL POINT SYSTEM EVALUATION

The bids that achieve 80% or more for the Functionality Evaluation will be further evaluated on Specific Goals whereby the Preference Point System of 80/20 with the maximum points as follows:

- Price = 80 points and 20 points are for preferential procurement requirements on Historically Disadvantaged Individuals (HDI).

Evaluation on Price and Historically Disadvantaged individual (HDI) will be calculated as per the below table;

Preferential points will be awarded in terms of the Historically Disadvantaged individual (HDI) which must be substantiated as follows (kindly refer to form SBD 6.1 for more details and fully complete to claim the points): -

Table 11: Specific Goals

Specific goals	**Points**	**Points Claimed** (to be completed by supplier)
Historically Disadvantaged individual (HDI)		
Enterprises with ownership of 51% or more by person/s who are black person/s.	**10**	
Enterprises with ownership of 51% or more by person/s who are women.	**5**	
Enterprises with ownership of 51% or more by person/s who are youth.	**3**	
Enterprise with ownership of 51% or more by person/s with disability.	**2**	
Enterprises with ownership of less than 51% by person/s who are black or less than 51% by person/s who are women or less than 51% by person/s who are youth or less than 51% by person/s with disability.	**0**	
Total	**20**	

TO SCORE FOR PREFERENCE POINTS, BIDDER MUST PROVIDE SUPPORTING INFORMATION (PROOF)THAT IS RELEVANT TO THE SPECIFIC GOALS.

Proof of specific goal claims (HDI ownership) is listed as returnable documents:

- Fully Completed & Signed SBD 6.1
- CIPC documents
- B-BBEE Certificate/ QSE/ EME Affidavit
- National Treasury Central Supplier Database copy (CSD)

27. ACCEPTANCE, HANDOVER AND OPERATIONAL READINESS

27.1. A site or service will not be regarded as accepted until the agreed acceptance tests have been completed and evidence has been approved by Legal Aid SA.

27.1.1. eLAA reachability and response under normal load

27.1.2. Internet speed and secure breakout

27.1.3. Microsoft 365 and Teams operation

27.1.4. 3CX voice quality where applicable

27.1.5. SD-WAN path selection and brownout handling

27.1.6. secondary-link failover and restoration

27.1.7. security policy enforcement

27.1.8. monitoring and automated incident generation

27.1.9. DR replication and recovery health for National office only

27.1.10. configuration backup and documentation completeness

27.2. Final project acceptance requires completion of the national rollout, DR readiness, outstanding-defect closure or approved defect plan, as-built documentation, operational training, service governance activation and agreed hypercare completion.

28. BID CONDITIONS

28.1. Bidders are encouraged to submit their bids in line with any attached annexures and detailed specifications, in order to facilitate a simplified fair and efficient evaluation process.

28.2. The bidders are required to submit one printed copy of the entire proposal and pricing as a separate file, accompanied by the exact same electronic copy of the entire submission and the pricing on a USB flash drive.

28.3. USB Flash Drive must include a protective cover and be labeled with Proposer's name and RFP number. Should the information on the USB not be consistent and identical to the hard copy, the hard copy shall prevail for purposes of evaluation.

28.4. Both printed submission and USB must be placed in the tender box on or before the closing date and time.

28.5. Legal Aid SA reserves the right to award the bid to one or more service providers.

28.6. Legal Aid SA reserves the right to award the bid in whole or only partially.

28.7. The General Conditions of Contract as stipulated by the National Treasury will be applicable.

28.8. Legal Aid SA reserves the right not to award the bid.

29. OBJECTIVE CRITERIA

29.1. In the event the recommended bidder is found to not satisfy/meet the conditions or requirements set hereunder, Legal Aid SA shall exercise its right in awarding the bid using applicable prescripts as provided for under the PPPFA, section 2(1)(f), which states, "the contract must be awarded to the tenderer who scores the highest points, unless objective criteria in addition to those contemplated in paragraphs (d) and (e) justify the award to another tenderer"

29.2. The recommended bidder must have a positive/good reputation which shall not jeopardize the reputation of Legal Aid SA.

29.3. The recommended bidder must have the financial ability to carry out the services as per the RFP requirements. Audited financials (will be requested from the recommended bidder prior to appointment), must be of sound applicable financial prescripts/industry standards.

29.4. The recommended bidder or its directors/shareholders must not have any pending criminal/civil cases instituted against them which may hinder the rendering of services if appointed to Legal Aid SA as per RFP requirements.

29.5. The recommended bidder or its personnel must not have a history of poor performance (e.g. negligence) or unethical conduct or employees who were dismissed/sanctioned for misconduct.

29.6. Legal Aid SA, like any other business, relies greatly on suppliers for most services, therefore, the interaction with suppliers/contractors/consultants can have a substantial impact on Legal Aid SA operations. Legal Aid SA can be negatively impacted by a supplier who does not have a good reputation or has been implicated in unethical activities, by association. To mitigate this reputational risk, Legal Aid SA will investigate any negative and positive news on the particular supplier/contractor/consultant before doing any business and will make an informed decision about its association.

29.7. In the event that the reference checks or processes conducted during a due diligence exercise for the recommended bidder, prior to appointment, should they yield negative feedback or operational risk to Legal Aid SA, the highest-scoring bidder may not be awarded the bid, and the second highest scoring bidder will be recommended for appointment provided its proposal meets the RFP requirements in all its respects.

30. ANNEXURES AND SCHEDULES

Annexure	Description
Annexure A	Final Legal Aid SA site list, address, site category, user count and bandwidth schedule
Annexure B	Pricing schedule - to be issued separately from the technical submission where the two-envelope process applies