Inquiry	Postbank Response
confirm whether we can participate together with a registered South African prime/partner to satisfy the local CSD, tax and B-BBEE requirements?	Bidders may participate through a consortium, joint venture, partnership or subcontracting arrangement where permitted by the RFP and applicable SCM requirements. The bid must clearly identify the prime/ accountable party and demonstrate compliance with all mandatory procurement and technical requirements
We would like to formally motivate that request respectfully ask Postbank to consider extending the closing date from 18 September 2026, 11:00, by one week to 25 September 2026, 11:00.	Granted. Refer to the RFP and any formal SCM addendum for the governing requirement
we kindly request an extension of two (2) weeks to the submission deadline to allow us sufficient time to complete the necessary technical and commercial assessments	The extension is approved. The revised closing date and time has been communicated through the formal SCM addendum/ notice, which prevails for all bidders
Are you looking to award one bidder as per the full scope of works? or can bidders bid as per their area/s of speciality only? With reference to the attached as per section 3 (scope of works).	Postbank intends to appoint one prime service provider for the full scope in Section 3. The prime may use approved partners/ subcontractors where permitted, but remains accountable for end-to-end delivery and compliance
Endpoint Security & EDR/XDR: Estimated total count of endpoints requiring agent deployment, broken down by workstations and servers.	For tender sizing, use an indicative baseline of up to 1,200 user endpoints and up to 200 servers. VM, cloud-workload and other designated endpoint quantities will be validated during mobilisation. The proposed licensing model must be scalable
Privileged Access Management (Sectona): Total number of administrative users.	For pricing, bidders should provide a scalable PAM model and clearly state the assumed quantity bands/ unit rates. Exact privileged-user, service-account, target-system and administrative-account inventories will be validated with the successful bidder during controlled discovery and are not disclosed in the open-bid clarification
How many end-users are within the current environment ?	For tender sizing and pricing, bidders may use an indicative baseline of up to 1,200 users/ identities. The final in-scope population will be validated with the successful bidder during mobilisation. Pricing must be scalable and clearly state unit-rate assumptions
How many endpoint devices are within the environment ?	For tender sizing, use an indicative baseline of up to 1,200 user endpoints and up to 200 servers. VM, cloud-workload and other designated endpoint quantities will be validated during mobilisation. The proposed licensing model must be scalable
Can the soc solution provided be in the form of a SOC as a service ?	Yes. A bidder-hosted managed SOC service is permissible provided it fully complies with the RFP, including South African hosting/data-residency requirements, Postbank real-time visibility and audit rights, logical segregation, service levels, incident-response obligations, and the contractual right for Postbank to relocate the SOC if required
Total employee, contractor and consultant headcount - needed to size MFA, SSO, DLP and awareness-training licensing	For tender sizing and pricing, bidders may use an indicative baseline of up to 1,200 users/ identities. The final in-scope population will be validated with the successful bidder during mobilisation. Pricing must be scalable and clearly state unit-rate assumptions
Total endpoint count (servers, workstations, laptops and virtual machines) - needed to size EDR/XDR licensing	For tender sizing, use an indicative baseline of up to 1,200 user endpoints and up to 200 servers. VM, cloud-workload and other designated endpoint quantities will be validated during mobilisation. The proposed licensing model must be scalable
ATM fleet size - needed to size endpoint and network security coverage	Do not rely on a fixed ATM quantity for base pricing unless specifically stated in the issued pricing schedule/ addendum. The solution must be capable of supporting designated ATM coverage where required. Detailed ATM inventory, platform and version information will be disclosed to the successful bidder under controlled access
Total mailbox count - needed to size email security and Microsoft 365 protection licensing	The environment uses Microsoft 365. Exact mailbox/licence populations will be validated during mobilisation. Where pricing depends on mailbox count, bidders must provide transparent scalable/ unit pricing and clearly state the quantity assumptions used
Number of privileged/administrative accounts - needed to size PAM	For pricing, bidders should provide a scalable PAM model and clearly state the assumed quantity bands/ unit rates. Exact privileged-user, service-account, target-system and administrative-account inventories will be validated with the successful bidder during controlled discovery and are not disclosed in the open-bid clarification
Please advise on the solutions currently being used to address the requirements and if there are any current service provider contracts and if so, the anticipated contract end date - needed to plan the transition-in timeline described in clause 9.	Postbank operates a brownfield/ hybrid security environment with existing internal capabilities, security technologies and third-party arrangements. Detailed OEMs, versions, topology, contractual dependencies and control configurations are security-sensitive and will be disclosed to the successful bidder under controlled access during mobilisation. Bidders must propose an interoperable, vendor-neutral approach and clearly identify assumptions
Have any specific OEM technologies been POC's or Demo'd leading to the writing of the RFB requirements.	No specific OEM product is prescribed by Postbank. Bidders must propose solutions that meet the functional, security, residency, interoperability and exit requirements in the RFP
Total employee, contractor and consultant headcount	For tender sizing and pricing, bidders may use an indicative baseline of up to 1,200 users/ identities. The final in-scope population will be validated with the successful bidder during mobilisation. Pricing must be scalable and clearly state unit-rate assumptions
Total endpoint count (servers, workstations, laptops and virtual machines)	For tender sizing, use an indicative baseline of up to 1,200 user endpoints and up to 200 servers. VM, cloud-workload and other designated endpoint quantities will be validated during mobilisation. The proposed licensing model must be scalable
ATM fleet size	Do not rely on a fixed ATM quantity for base pricing unless specifically stated in the issued pricing schedule/ addendum. The solution must be capable of supporting designated ATM coverage where required. Detailed ATM inventory, platform and version information will be disclosed to the successful bidder under controlled access
Total mailbox count	The environment uses Microsoft 365. Exact mailbox/licence populations will be validated during mobilisation. Where pricing depends on mailbox count, bidders must provide transparent scalable/ unit pricing and clearly state the quantity assumptions used
Number of privileged/administrative accounts	For pricing, bidders should provide a scalable PAM model and clearly state the assumed quantity bands/ unit rates. Exact privileged-user, service-account, target-system and administrative-account inventories will be validated with the successful bidder during controlled discovery and are not disclosed in the open-bid clarification
IT was mentioned in the briefing that Postbank will keep the existing HSM, this contradicts point 3.6 – please confirm if the HSM should be provided or not and if not would the management of the existing tech be out of scope for this contract, if a new HSM is to be positioned, would a cloud model be acceptable or only physical hardware?	Postbank has existing HSM capability that will be retained for the base scope. Bidders should not assume wholesale HSM replacement. The required scope is integration, security monitoring/ assurance and support of the applicable cryptographic-control requirements. Detailed HSM make/model, topology, key-management design and ceremony information will be disclosed only to the successful bidder under controlled access

Please advise on the solutions currently being used to address the requirements and if there are any current service provider contracts and if so, the anticipated contract end date	Postbank operates a brownfield/ hybrid security environment with existing internal capabilities, security technologies and third-party arrangements. Detailed OEMs, versions, topology, contractual dependencies and control configurations are security-sensitive and will be disclosed to the successful bidder under controlled access during mobilisation. Bidders must propose an interoperable, vendor-neutral approach and clearly identify assumptions
we thus request an additional 2 weeks extension from the current 18th September closing date be considered.	The extension is approved. The revised closing date and time has been communicated through the formal SCM addendum/ notice, which prevails for all bidders
Will POSTBANK provide estimated quantities for pricing purposes, including the number of users, endpoints, servers, privileged accounts, ATMs, cloud workloads, and log ingestion volumes required under the contract.	For tender sizing and pricing, bidders may use an indicative baseline of up to 1,200 users/ identities. The final in-scope population will be validated with the successful bidder during mobilisation. Pricing must be scalable and clearly state unit-rate assumptions
In developing the proposed solution, may bidders assume that POSTBANK will provide and fund any additional Microsoft licences, feature upgrades, or service add-ons required to support the bidder's solution where these form part of POSTBANK's existing Microsoft estate (e.g., Microsoft Defender for Cloud, Entra ID P2, etc.)? This clarification is requested as POSTBANK already holds a direct contractual relationship with Microsoft for the procurement and management of Microsoft software and cloud services.	Bidders must include and clearly price all licences, add-ons and subscriptions necessary for their proposed solution to meet the RFP. Existing Postbank entitlements may be leveraged where confirmed during mobilisation, but bidders must not assume that Postbank will fund unpriced dependencies
The POSTBANK has provided Bidders with a pricing table as part of Section 5. Is completion of this pricing table by the Bidder sufficient to meet the requirements of Section 5 (bullet 1) for a detailed pricing breakdown?	The requirement is governed by the issued RFP. Any detailed current-state information that is not expressly included in the RFP will be provided to the successful bidder during controlled mobilisation where necessary for delivery. Bidders should state all assumptions used for pricing and solution design
Where solutions are licensed or charged based on consumption (e.g., SIEM log volume, cloud storage, data retention, threat intelligence feeds), should bidders price based on current usage, projected growth, or a defined baseline provided by POSTBANK?	Bidders must use the tender sizing information as the evaluation baseline, state all assumptions, and provide transparent scalable/unit pricing for consumption-driven components. Final consumption baselines will be validated during mobilisation and any changes will follow the approved contract/ change-control mechanism
For evaluation and comparative pricing purposes, does POSTBANK require bidders to use a specified exchange rate when preparing their proposals? This would ensure that variations in foreign exchange assumptions do not influence the comparison of bidder pri	Service-specific criticality, RTO/RPO values and recovery priorities are security-sensitive and will be confirmed with the successful bidder during controlled mobilisation. Bidders must demonstrate capability to support risk-based recovery tiers and the service-specific recovery windows required by Postbank
Please confirm the expected billing and payment model, as well as the payment terms.	Monthly
In the provided pricing table, the Bidder is required to insert quantities. Where the Bidder is proving that line item as a service, should we insert a quantity of 1?	The requirement is governed by the issued RFP. Any detailed current-state information that is not expressly included in the RFP will be provided to the successful bidder during controlled mobilisation where necessary for delivery. Bidders should state all assumptions used for pricing and solution design
Does POSTBANK require pricing to remain fixed for the full three-year contract term, or will annual CPI adjustments and foreign exchange fluctuations be permitted?	Pricing must comply with the commercial terms issued by SCM. Bidders should submit the required three-year pricing and clearly disclose any proposed escalation assumptions. no escalation or foreign-exchange adjustment should be assumed unless expressly permitted in the final bid/ contract terms
For evaluation and comparative pricing purposes, does POSTBANK require bidders to use a specified exchange rate when preparing their proposals? This would ensure that variations in foreign exchange assumptions do not influence the comparison of bidder pricing.	Service-specific criticality, RTO/ RPO values and recovery priorities are security-sensitive and will be confirmed with the successful bidder during controlled mobilisation. Bidders must demonstrate capability to support risk-based recovery tiers and the service-specific recovery windows required by Postbank
How many endpoints does POSTBANK have, that would need to be included for End-point security monitoring?	1200
How many servers would require hardening?	For tender sizing, use an indicative baseline of up to 200 servers. The final server/ VM population will be validated during mobilisation and the bidder must provide scalable unit pricing
What cloud environments does POSTBANK currently make use of (AWS, Azure, Google Cloud)	Postbank operates a hybrid environment that includes public-cloud services. Bidders must demonstrate capability across the cloud platforms specified in the RFP. Detailed workload inventory, tenancy and architecture will be provided to the successful bidder during controlled discovery
Does Postbank have an existing Zero Trust strategy?	Postbank will not disclose detailed control-state, maturity gaps or defensive configuration information during the open-bid clarification. Bidders should assume a brownfield environment and propose discovery, integration and uplift activities consistent with the RFP. Detailed current-state information will be provided to the successful bidder under controlled access
Please provide an overview of the current technology landscape, including On-premises infrastructure, Cloud environments (Azure, AWS, Google Cloud), End-user computing devices, Datacentres.	Postbank operates a hybrid environment that includes public-cloud services. Bidders must demonstrate capability across the cloud platforms specified in the RFP. Detailed workload inventory, tenancy and architecture will be provided to the successful bidder during controlled discovery
What cloud environments does POSTBANK currently make use of (AWS, Azure, Google Cloud)	Postbank operates a hybrid environment that includes public-cloud services. Bidders must demonstrate capability across the cloud platforms specified in the RFP. Detailed workload inventory, tenancy and architecture will be provided to the successful bidder during controlled discovery
What firewall platforms are currently in use?	Postbank operates a brownfield/hybrid security environment with existing internal capabilities, security technologies and third-party arrangements. Detailed OEMs, versions, topology, contractual dependencies and control configurations are security-sensitive and will be disclosed to the successful bidder under controlled access during mobilisation. Bidders must propose an interoperable, vendor-neutral approach and clearly identify assumptions
What IAM platform does POSTBANK currently use?	Postbank operates a brownfield/ hybrid security environment with existing internal capabilities, security technologies and third-party arrangements. Detailed OEMs, versions, topology, contractual dependencies and control configurations are security-sensitive and will be disclosed to the successful bidder under controlled access during mobilisation. Bidders must propose an interoperable, vendor-neutral approach and clearly identify assumptions
Is Network Access Control (NAC) currently deployed within POSTBANK?	Postbank will not disclose detailed control-state, maturity gaps or defensive configuration information during the open-bid clarification. Bidders should assume a brownfield environment and propose discovery, integration and uplift activities consistent with the RFP. Detailed current-state information will be provided to the successful bidder under controlled access
How many of the following are considered in-scope for this service solution a.Users b.Endpoints c.Servers d.Applications e.Cloud workloads f.Network Zones	Postbank operates a hybrid environment that includes public-cloud services. Bidders must demonstrate capability across the cloud platforms specified in the RFP. Detailed workload inventory, tenancy and architecture will be provided to the successful bidder during controlled discovery
Are there any critical legacy systems in the scope that cannot support modern authentication and access controls?	None

Is the ATM environment included within the scope of Zero Trust?	Do not rely on a fixed ATM quantity for base pricing unless specifically stated in the issued pricing schedule/ addendum. The solution must be capable of supporting designated ATM coverage where required. Detailed ATM inventory, platform and version information will be disclosed to the successful bidder under controlled access
What identity platform(s) are currently deployed (e.g. Active Directory, Microsoft Entra ID)?	Postbank operates a brownfield/ hybrid security environment with existing internal capabilities, security technologies and third-party arrangements. Detailed OEMs, versions, topology, contractual dependencies and control configurations are security-sensitive and will be disclosed to the successful bidder under controlled access during mobilisation. Bidders must propose an interoperable, vendor-neutral approach and clearly identify assumptions
Is Multi-Factor Authentication currently implemented across the organisation?	Yes. Refer to the RFP and any formal SCM addendum for the governing requirement
Are third-party users, contractors, and service providers included within scope?	Yes. Refer to the RFP and any formal SCM addendum for the governing requirement
Are machine identities and service accounts required to be included in the Zero Trust model?	For pricing, bidders should provide a scalable PAM model and clearly state the assumed quantity bands/ unit rates. Exact privileged-user, service-account, target-system and administrative-account inventories will be validated with the successful bidder during controlled discovery and are not disclosed in the open-bid clarification
What WAN network is currently deployed e.g SD-WAN?	Postbank operates a brownfield/ hybrid security environment with existing internal capabilities, security technologies and third-party arrangements. Detailed OEMs, versions, topology, contractual dependencies and control configurations are security-sensitive and will be disclosed to the successful bidder under controlled access during mobilisation. Bidders must propose an interoperable, vendor-neutral approach and clearly identify assumptions
Is data classification already implemented?	Postbank will not disclose detailed control-state, maturity gaps or defensive configuration information during the open-bid clarification. Bidders should assume a brownfield environment and propose discovery, integration and uplift activities consistent with the RFP. Detailed current-state information will be provided to the successful bidder under controlled access
Are Data Loss Prevention (DLP) controls currently deployed?	Yes. Refer to the RFP and any formal SCM addendum for the governing requirement
Which regulatory and compliance frameworks must be supported?	The required frameworks are those specified in the RFP, including applicable SARB cyber-resilience requirements, POPIA, PCI DSS/ PCI PIN where applicable, ISO/ IEC 27001 and other applicable payment/ regulatory obligations
What reporting and audit requirements are expected?	Bidders must meet the reporting, audit-evidence and transparency requirements in Sections 3, 7, 8 and the SLA schedule, including monthly operational reporting, quarterly executive/risk reporting and timely audit/regulatory evidence
Will the Bidder be responsible for user onboarding/offboarding and access administration?	Postbank retains business ownership of joiner/ mover/ leaver authorisation. The successful bidder must support the security tooling, control enforcement, monitoring and integration required by the RFP, with detailed RACI agreed during mobilisation
Will the Bidder be responsible for policy management and change management activities?	Postbank retains governance and approval authority for security policy and change management. The bidder is responsible for proposing, implementing and operating approved security-control changes within the contracted scope and Postbank's change-control process
Is the bidder responsible for remediation and implementation of controls, or only monitoring and governance?	The bidder is not limited to monitoring. Within the contracted cybersecurity scope, the bidder must implement and operate required controls and drive remediation to closure, while coordinating with Postbank technology owners for changes that require Postbank-owned system or application action
Does Postbank anticipate that the Bidder would operate and administer the Zero Trust technologies and associated identity and network controls, or only provide monitoring, governance and security operations services?	Yes. Refer to the RFP and any formal SCM addendum for the governing requirement
What responsibilities remain with Postbank's infrastructure, cloud, and application teams?	Postbank retains accountability for cybersecurity strategy, risk acceptance, regulatory reporting, business/ system ownership and change approval. The successful bidder is accountable for delivery and operation of the contracted security services, with a detailed RACI to be agreed during mobilisation
Which applications, platforms and user populations are in scope for Identity Governance and Administration?	Postbank will provide the successful bidder with the detailed Identity Governance and Administration (IGA) scope and baseline inventory during the mobilisation/transition phase.
What specific regulatory, audit and segregation-of-duties requirements must be enforced across the banking environment?	SARB,PASA PCI DSS
How many identities will be managed?	For tender sizing and pricing, bidders may use an indicative baseline of up to 1,200 users/identities. The final in-scope population will be validated with the successful bidder during mobilisation. Pricing must be scalable and clearly state unit-rate assumptions.
Which system is the authoritative source of identity data?	AD and Entra
Are Joiner-Mover-Leaver (JML) processes currently automated?	No. Refer to the RFP and any formal SCM addendum for the governing requirement.
Which applications must be connected to the IGA platform?	AD and Entra
Are there any legacy or custom-developed banking applications?	Postbank will not disclose detailed control-state, maturity gaps or defensive configuration information during the open-bid clarification. Bidders should assume a brownfield environment and propose discovery, integration and uplift activities consistent with the RFP. Detailed current-state information will be provided to the successful bidder under controlled access.
Which systems require Segmentation of Duties (SoD) controls?	Core banking and transactional systems,
Are there banking-specific roles that must be monitored?	Previlledge roles
Is MFA currently deployed? If so, which MFA solution is in use today?	Postbank will not disclose detailed control-state, maturity gaps or defensive configuration information during the open-bid clarification. Bidders should assume a brownfield environment and propose discovery, integration and uplift activities consistent with the RFP. Detailed current-state information will be provided to the successful bidder under controlled access.
Must MFA be enforced for all users or only high-risk groups?	Yes. Refer to the RFP and any formal SCM addendum for the governing requirement.
Are there any POSTBANK applications that do not currently support MFA?	No. Refer to the RFP and any formal SCM addendum for the governing requirement.
Which applications require Single Sign On (SSO) integration?	No. Refer to the RFP and any formal SCM addendum for the governing requirement.
Are there legacy applications requiring custom federation?	Yes. Refer to the RFP and any formal SCM addendum for the governing requirement.
Are there non-Windows platforms requiring integration?	Yes. Refer to the RFP and any formal SCM addendum for the governing requirement.
What is the expected incident response SLA?	The SLA will be discussed during the contracting stage
Are there SARB requirements that must be considered?	Yes. Refer to the RFP and any formal SCM addendum for the governing requirement.
Are POPIA reporting requirements applicable?	Yes. Refer to the RFP and any formal SCM addendum for the governing requirement.
What core banking platform is being used?	Such would be communicated in during the contracting phase
Does the core banking platform support SAML/OIDC integration?	Such would be communicated in during the contracting phase
Can MFA be integrated with the POSTBANK banking applications?	Yes. Refer to the RFP and any formal SCM addendum for the governing requirement.

Does the banking platform support automated provisioning and deprovisioning?	Yes. Refer to the RFP and any formal SCM addendum for the governing requirement.
Does the platform support role-based access controls?	Yes. Refer to the RFP and any formal SCM addendum for the governing requirement.
How many users require awareness training and phishing simulation?	weekly
What frequency of phishing simulations is required?	weekly
Is the bidder expected to conduct social engineering assessments, including vishing and physical assessments?	Yes. Refer to the RFP and any formal SCM addendum for the governing requirement.
Does Postbank currently have an Insider Threat Programme?	Yes. Refer to the RFP and any formal SCM addendum for the governing requirement.
What systems and data sources must be monitored for insider threats?	Core banking system
Is endpoint, email, and cloud DLP required?	Yes. Refer to the RFP and any formal SCM addendum for the governing requirement.
What user risk scoring and UEBA capabilities are expected?	POSTBANK requires the proposed solution to provide User and Entity Behaviour Analytics (UEBA) and risk-scoring capabilities as part of the cybersecurity monitoring and detection capability.
What reporting metrics and dashboards are required?	The proposed solution should provide operational, management, risk, compliance and executive-level dashboards and reporting covering the cybersecurity services and technologies within the scope of the tender
Is awareness training required in multiple languages?	only english
Are there regulatory awareness requirements specific to Postbank?	Yes , regulatory awareness is mandatory
What data classification framework is currently used?	Postbank will not disclose detailed control-state, maturity gaps or defensive configuration information during the open-bid clarification. Bidders should assume a brownfield environment and propose discovery, integration and uplift activities consistent with the RFP. Detailed current-state information will be provided to the successful bidder under controlled access.
Which metrics must be reported quarterly?	Monthly ,security incidents, threat detection and soc perfomance, vulnerability management ,Identity and access security
Does Postbank currently use Mimecast Awareness Training or another awareness platform?	Yes. Refer to the RFP and any formal SCM addendum for the governing requirement.
Does Postbank already own Microsoft Purview licensing?	Yes. Refer to the RFP and any formal SCM addendum for the governing requirement.
How many users and mailboxes are in scope for the service?	The environment uses Microsoft 365. Exact mailbox/licence populations will be validated during mobilisation. Where pricing depends on mailbox count, bidders must provide transparent scalable/unit pricing and clearly state the quantity assumptions used.
Is the email environment Exchange Online, Exchange on-premises, or hybrid?	Hybrid
How many email domains are in scope?	two
What email archiving retention period is required?	The retention period will be confirmed by POSTBANK during the requirements-confirmation/implementation phase and will be aligned with applicable legislation, regulatory requirements and POSTBANK's approved records-retention policy
What legal hold and eDiscovery requirements must be supported?	To support eDiscovery capabilities for authorized investigations, litigation, regulatory requests, internal investigations and other legally permissible purposes.
Is the bidder expected to provide email journaling services?	Yes. The bidder is expected to provide email journaling capability as part of the proposed email security and archiving solution.
Is DLP required across Email, SharePoint, OneDrive, Teams, and endpoints?	Yes. POSTBANK requires Data Loss Prevention (DLP) capabilities across the applicable Microsoft 365 services and supported endpoint environments within the scope of the tender.
Does Postbank currently have any email security, archiving, DLP or collaboration security solutions that must be retained or integrated?	Yes. POSTBANK currently has Mimecast within its email-security environment. The proposed solution must take into consideration the existing environment and provide for appropriate integration, migration, coexistence and/or transition as applicable to the proposed solution.
What incident response and restoration SLAs are required for email and communication security incidents?	POSTBANK requires the bidder to provide 24x7x365 monitoring, incident response and escalation for email and communication security incidents within the scope of the service
What reporting, compliance and regulatory requirements must the solution support?	The proposed solution must provide reporting, monitoring and audit capabilities sufficient to support POSTBANK's internal governance, risk management, audit and applicable regulatory and compliance obligations
How many servers, endpoints, network devices, databases, applications, and cloud workloads are in scope?	For tender sizing, use an indicative baseline of up to 200 servers. The final server/VM population will be validated during mobilisation and the bidder must provide scalable unit pricing.
Which operating systems and platforms are in scope (Windows, Linux, UNIX, macOS, virtual infrastructure, etc.)?	Windows and Linux
Which cloud environments are included in scope (Azure, AWS, GCP, private cloud, SaaS platforms)?	Postbank operates a hybrid environment that includes public-cloud services. Bidders must demonstrate capability across the cloud platforms specified in the RFP. Detailed workload inventory, tenancy and architecture will be provided to the successful bidder during controlled discovery.
Does Postbank currently have a patch management solution in place?	Yes. Refer to the RFP and any formal SCM addendum for the governing requirement.
Is the bidder responsible for performing all remediation activities?	Yes. Refer to the RFP and any formal SCM addendum for the governing requirement.
Does the requirement to remediate critical vulnerabilities within seven days apply to all critical findings or only those deemed exploitable?	Yes. Refer to the RFP and any formal SCM addendum for the governing requirement.
What change management processes and maintenance windows must be followed when deploying patches?	2 weeks
Are there any systems that cannot be patched due to operational, vendor, or business constraints?	Such would be communicated in during the contracting phase
Is authenticated vulnerability scanning required across all systems and environments?	Yes. Refer to the RFP and any formal SCM addendum for the governing requirement.
Will Postbank provide the necessary credentials and privileged access required for authenticated scanning?	Yes. Refer to the RFP and any formal SCM addendum for the governing requirement.
What frequency is required for vulnerability assessments and scanning activities?	POSTBANK requires vulnerability assessment and scanning activities to be performed on a risk-based and recurring basis to provide continuous visibility of vulnerabilities across the in-scope technology environment.
Must vulnerability assessments cover internal systems, external systems, applications, databases, cloud environments, and network devices?	Postbank operates a hybrid environment that includes public-cloud services. Bidders must demonstrate capability across the cloud platforms specified in the RFP. Detailed workload inventory, tenancy and architecture will be provided to the successful bidder during controlled discovery.
What is the required scope of the quarterly penetration testing (external infrastructure, internal network, web applications, APIs, mobile applications, cloud platforms, etc.)?	Postbank operates a hybrid environment that includes public-cloud services. Bidders must demonstrate capability across the cloud platforms specified in the RFP. Detailed workload inventory, tenancy and architecture will be provided to the successful bidder during controlled discovery.
How many internet-facing IP addresses, applications, domains, and services are included in the penetration testing scope?	Detailed architecture, topology, technology versions and security configurations will be provided only to the successful bidder under controlled access during mobilisation. The bid should be based on the functional and non-functional requirements in the RFP and clearly stated assumptions.
What reporting, SLA, KPI, and executive dashboard requirements must be supported for vulnerability management and remediation activities?	POSTBANK requires the proposed vulnerability-management solution to provide operational, management, risk and executive-level reporting and dashboards covering the complete vulnerability lifecycle from identification through remediation and validation.

In the SLA requirements, POSTBANK indicated that the Penetration Testing Frequency should be at least twice per year. However, in 3.14 Patch and Vulnerability Management, it is stated that penetration testing must be done quarterly. Could POSTBANK please confirm which is correct?	Bidders must provide penetration testing at least twice per year as the minimum SLA baseline, with additional testing after material changes, significant incidents, regulatory/audit requirements or where directed by Postbank. The final testing calendar will be agreed during mobilisation.
How many Microsoft Windows End-user Devices do you have?	The current Microsoft Windows end-user device inventory will be validated and confirmed during the requirements-confirmation and mobilisation phase.
How many Apple MAC Devices do you have ?	12
How Many windows Servers do you have?	200
How Many Linux Servers do you have?	50
How many ATM's do you have?	Do not rely on a fixed ATM quantity for base pricing unless specifically stated in the issued pricing schedule/addendum. The solution must be capable of supporting designated ATM coverage where required. Detailed ATM inventory, platform and version information will be disclosed to the successful bidder under controlled access.
What operating system does your ATM's run on ?	Do not rely on a fixed ATM quantity for base pricing unless specifically stated in the issued pricing schedule/addendum. The solution must be capable of supporting designated ATM coverage where required. Detailed ATM inventory, platform and version information will be disclosed to the successful bidder under controlled access.
How many physical firewalls do you have ?	N/A
How many routers do you have ?	N/A
How many switches do you have ?	N/A
How many remote locations do you have ?	POSTBANK has multiple remote/branch locations that require connectivity to the central technology environment. The current number of active remote locations will be validated and confirmed during the requirements-confirmation and mobilisation phase.
How do Braches communicate over the wan e.g. MPLS / Private APN ?	APN
What is the expected retention requirements for the security logs?	6 months live and 12 months offline and 5 years offside
Do you have mainframes, and if yes what OEM and how many ?	None
How many API end points do you have ?	Such would be communicated in during the contracting phase
Do you use public cloud services, if yes please provide a list ?	Yes. POSTBANK makes use of public cloud services, with Amazon Web Services (AWS) being a key cloud platform within the current environment.
What do you currently use for identity and access management ?	POSTBANK currently uses Microsoft Active Directory (AD) as a core identity and access-management platform for user authentication, account management and access control across the applicable technology environment.
Please provide a list of sites and the WAN link sizes per site	POSTBANK operates across multiple geographically distributed sites, including branches, offices and other operational locations. The detailed site inventory and WAN bandwidth information will be validated and confirmed during the requirements-confirmation and mobilisation phase.
How many applications do you have e.g. Core Banking ?	None
Can you provide a list of database technologies in use e.g. MSSQL, number of database engine instances and number of databases?	MSQL and Oracle
How many email boxes do you have that relate to actual people ?	200
How many email boxes do you have that are generic e.g. meeting rooms, shared mail accounts ?	POSTBANK has a number of shared, generic and resource mailboxes, including mailboxes used for business functions, departments, service accounts, meeting rooms and other shared operational purposes.
How do remote users access the systems e.g. VPN and how many remote users ?	VPN
How do third party's access the Banks applications ?	VPN
What code repository do you use?	Postbank currently doesn't have in-house development
How many lines of code do you have ?	Postbank currently doesn't have in-house development
How many lines of code do you develop in addition to the base code base per month ?	Postbank currently doesn't have in-house development
How many applications are internet facing to the public ?	POSTBANK has a number of publicly accessible/internet-facing applications and services. The current inventory and exact number of internet-facing applications will be validated and confirmed during the requirements-confirmation and mobilisation phase.
What programming languages have been used for application development ?	Postbank currently doesn't have in-house development
What 3rd party application integrations are being used ?	POSTBANK's technology environment includes integrations with a number of third-party and externally provided applications, platforms and services supporting business operations, infrastructure, security and financial services.
Do you use an integration service bus / iPass, if yes what technology is being used and where is it deployed ?	None
What is the Banks RTO and RPO requirements in terms of Cyber recovery not in terms of IT continuity?	Service-specific criticality, RTO/RPO values and recovery priorities are security-sensitive and will be confirmed with the successful bidder during controlled mobilisation. Bidders must demonstrate capability to support risk-based recovery tiers and the service-specific recovery windows required by Postbank.
What is the size of the front end data that needs to be protected?	The total volume of front-end data requiring protection will be validated during the requirements-confirmation and mobilisation phase.
What is the retention period required for backup data ?	backup data to be retained in accordance with its approved information-retention, backup, cyber-recovery, regulatory and business requirements.
Do you have a prod and DR DC facility, how far apart are they from each other and what is the bandwidth?	Yes. POSTBANK has Production and Disaster Recovery (DR) environments. The environments are designed to support business continuity, disaster recovery and cyber-recovery requirements,The detailed physical distance between the Production and DR facilities and the inter-site bandwidth will be confirmed during the requirements-confirmation and mobilisation phase, subject to applicable security and information-disclosure requirements.
Does the Recovery Assurance Capability cover the JV's services (If bidding as a JV) or Postbank's entire environment?	The Recovery Assurance Capability is required to support POSTBANK's in-scope environment and services covered by this contract, including services delivered by a Joint Venture (JV), consortium or other contracted service providers.
Kindly Confirm if affidavits are acceptable for client references, as financial institutions are often reluctant to provide letters.	Yes. Affidavits may be accepted as supporting evidence for client references, particularly where the client is unable or unwilling to issue a formal reference letter due to its internal policies or confidentiality requirements.
Please confirm if these timeframes are indicative and if we can propose our own roadmap	The timeframes specified in the tender should be regarded as minimum implementation milestones and target timeframes, rather than preventing bidders from proposing a detailed implementation roadma
Please clarify what is meant by this statement "Postbank reserves the right to relocate the SOC to its own premises at any stage during the contract. Should Postbank elect to do so, no hosting fees shall be payable for bidder- provided facilities"	The relocation clause applies to the contracted SOC service capability. Detailed personnel, platform, facility, licence-transfer and commercial arrangements will be agreed with the successful bidder through an approved transition plan and change-control process. Bidders must identify any portability or residual-cost constraints in their proposals.

states that Postbank or its agent will run vulnerability scans and propose remediation, while the bidder closes vulnerabilities within SLA. Section 3.14 requires the bidder to conduct continuous vulnerability assessments and authenticated scanning. Which party owns scanning, and which owns remediation execution?	the successful bidder will be responsible for conducting the vulnerability assessment and scanning activities required under Section 3.14, including continuous vulnerability assessment, authenticated scanning where technically feasible, external/perimeter scanning and the other scanning activities defined in the scope
Requires quarterly penetration testing. the SLA table in Section 6 states penetration testing is conducted at least twice per year. Which frequency governs?	Bidders must provide penetration testing at least twice per year as the minimum SLA baseline, with additional testing after material changes, significant incidents, regulatory/audit requirements or where directed by Postbank. The final testing calendar will be agreed during mobilisation.
Fixes the commercial split at 90/10, but SBD 6.1 states "80/20 or 90/10". Please confirm the estimated contract value band and the definitive preference point system.	The 90/10 preference point system shall apply
Requires certification or formal partnership with three of: ISO 27001, PCI DSS QSA, CISSP, CEH, OSCP. These mix organisational certifications with individual ones. Please confirm whether a combination is acceptable, and note that a QSA firm is ordinarily precluded from assessing an environment it operates - how does Postbank intend to manage that independence conflict?	POSTBANK confirms that a combination of organisational certifications and appropriately qualified individual certifications is acceptable, provided that the bidder demonstrates that the required capabilities are available within its proposed delivery team and/or through a formally established partnership,Organisational certifications/accreditations, where applicable, such as ISO/IEC 27001 and PCI DSS QSA capability. andIndividual professional certifications, such as CISSP, CEH and OSCP, held by personnel proposed for the relevant services.
Requires a resource "certified as CISO". Is this the EC-Council C|CISO specifically, or will CISM, CISSP-ISSMP or equivalent be accepted?	The resource must be a certified CISO, and another resource must be CISSP certified
Asks for a PCI DSS Report on Compliance. ROCs are confidential and rarely released. Will an Attestation of Compliance (AOC) be accepted in its place?	Yes. POSTBANK confirms that a valid PCI DSS Attestation of Compliance (AOC) must submitted in place of the full PCI DSS Report on Compliance (ROC), where the ROC is subject to confidentiality or contractual restrictions
What is the total endpoint count, split by servers, workstations, laptops, virtual machines, and cloud workloads?	For tender sizing, use an indicative baseline of up to 1,200 user endpoints and up to 200 servers. VM, cloud-workload and other designated endpoint quantities will be validated during mobilisation. The proposed licensing model must be scalable.
What is the total ATM estate size, and what operating systems and OEM platforms are in use (NCR, Diebold, other)? Does the ATM management contract permit third-party EDR agents?	Do not rely on a fixed ATM quantity for base pricing unless specifically stated in the issued pricing schedule/addendum. The solution must be capable of supporting designated ATM coverage where required. Detailed ATM inventory, platform and version information will be disclosed to the successful bidder under controlled access.
What is the total user headcount (employees, contractors, third parties) for MFA, awareness training and phishing simulation sizing?	1200
What is the total user headcount (employees, contractors, third parties) for MFA, awareness training and phishing simulation sizing?	The exact total user headcount, comprising employees, contractors and applicable third-party users, will be validated and confirmed during the requirements-confirmation and mobilisation phase.
What is the estimated SIEM ingest volume in EPS and GB/day, and the number and type of log sources? How many require custom parsers (legacy, mainframe, core banking, proprietary applications)?	For indicative tender sizing, bidders may use a baseline of approximately 100 EPS, with scalable pricing for growth. Exact log-source inventory, peak rates, daily volume, retention tiers and onboarding priorities will be validated with the successful bidder during mobilisation. Bidders must state all sizing and retention assumptions.
What is the required SIEM log retention - hot, warm and cold - and over what period? PCI DSS sets a 12-month floor. please confirm Postbank's actual requirement, as this materially drives storage cost.	POSTBANK requires SIEM log retention to comply with applicable regulatory, audit, security and internal information-retention requirements. The 12-month PCI DSS retention requirement should be treated as the minimum baseline for applicable PCI DSS log
How many privileged, service and application accounts are in scope for PAM? How many AD forests/domains exist, and is the identity estate on-premises, Entra-only, or hybrid?	For pricing, bidders should provide a scalable PAM model and clearly state the assumed quantity bands/unit rates. Exact privileged-user, service-account, target-system and administrative-account inventories will be validated with the successful bidder during controlled discovery and are not disclosed in the open-bid clarification.
How many physical sites, branches and data centres are in scope, and what is the available bandwidth at each for log shipping?	POSTBANK has multiple physical locations, including branches, offices, operational sites and data-centre environments that may be relevant to the SIEM/log-collection architecture,The exact number of sites in scope and the available WAN bandwidth at each location have not been finalised for tender sizing purposes and will be validated during the requirements-confirmation and mobilisation phase.The proposed solution must support log collection from geographically distributed locations and accommodate the available network connectivity between branches/sites, data centres, cloud environments and the SOC/SIEM platform
Which core banking, payment switch and card management platforms are in use, who hosts them, and are they under third-party managed service arrangements?	POSTBANK operates core banking, payment, transactional and card-related technology platforms within its environment. These include core banking/transaction-processing systems, payment and settlement platforms, databases, application middleware and supporting infrastructure.The detailed platform names, versions, hosting locations, architecture and service-provider arrangements will be validated and provided during the requirements-confirmation and mobilisation phase, subject to applicable security and information-disclosure controls.
Is this a greenfield or brownfield deployment? Please provide an inventory of incumbent security tooling (SIEM, EDR, PAM, DLP, email gateway, firewalls, WAF) with licence expiry dates.	The proposed deployment should be regarded as a brownfield environment, as POSTBANK has an existing cybersecurity technology estate and operational security capabilities. The successful bidder will therefore be required to integrate with, transition from, coexist with, or replace existing technologies as applicable to the final solution and approved transition plan
Are any existing licences transferable to the incoming provider, or must all tooling be priced as new?	Bidders must identify the proposed licence ownership model and any OEM transfer restrictions. Postbank requires full portability of its data, configurations, rules, workflows and Postbank-specific content at exit. OEM licence transferability will be governed by the applicable OEM terms and the final contract. no undisclosed lock-in is acceptable.
Is there an incumbent MSSP, and will a parallel-run period be required? If so, who bears the dual-running cost?	A parallel-run/coexistence period may be required to ensure continuity of security monitoring, detection, incident response, log coverage and operational services during transition from incumbent arrangements to the successful bidder.The duration and scope of any parallel run will be determined during the mobilisation and transition planning phase, based on the final solution, service scope, technology migration requirements, risk assessment and agreed transition plan.
Must historical log data be migrated into the new SIEM, and if so, what volume and period?	Historical log migration into the new SIEM is not necessarily required for the entire historical dataset. The requirement will be determined during the transition and requirements-confirmation phase based on regulatory, audit, investigation, cyber-security and operational requirements.Where historical logs are required to be migrated, the successful bidder will be required to support the secure migration and/or controlled access to the relevant historical data, subject to technical feasibility and the capabilities of the incumbent platform.
Does Postbank maintain a CMDB or authoritative asset inventory? The 95% log-coverage and 95% EDR-coverage SLAs require an agreed baseline - how will "critical agreed assets" be defined and by when?	POSTBANK maintains asset and configuration information across its technology environment. however, the authoritative in-scope asset baseline for the new SOC services will be validated and agreed during the requirements-confirmation and mobilisation phase.
What is the intended contract commencement date, and does "Month 1" in the deployment roadmap run from contract signature or from completion of transition-in?	The mobilisation/deployment clock will commence from the contractual commencement date stated in the final agreement/appointment documentation, subject to Postbank making agreed prerequisites reasonably available. Detailed dependencies and milestone acceptance will be baselined at kickoff.

Deploying EDR, MFA, email security and PAM across the full estate within Month 1 is aggressive. Will Postbank accept a defined critical-asset subset for Month 1, with full-estate rollout phased thereafter?	POSTBANK recognises that deployment of EDR, MFA, email security and PAM across the full estate within Month 1 may require a phased implementation approach, particularly where integration, legacy platforms, third-party dependencies, change-management requirements or technical constraints apply.POSTBANK will therefore accept a risk-based phased rollout, provided that the bidder demonstrates a clear and achievable implementation plan.During Month 1, priority should be given to critical and high-risk assets, users and services, including where applicable
Section 5.4 prohibits storage or replication of regulated data outside South Africa, while Sections 3.2 and 3.15 require Microsoft 365 protection and multi-cloud CSPM/CWPP across AWS, Azure and GCP. Microsoft security telemetry and several leading SaaS security platforms have no South African data residency option. How does Postbank wish this to be reconciled - narrower tooling choice, a defined telemetry exclusion, or a documented risk acceptance?	POSTBANK's requirement is that regulated data subject to Section 5.4 must not be stored or replicated outside South Africa. This requirement takes precedence over the bidder's preferred technology architecture.POSTBANK does not intend to automatically exclude Microsoft 365 security capabilities, multi-cloud CSPM/CWPP or other leading security technologies where their control-plane or telemetry architecture has global components. However, bidders must demonstrate how their proposed solution will comply with POSTBANK's data-residency and regulatory requirements.
Does the residency requirement extend to OEM vendor support and follow-the-sun escalation, which typically involves offshore engineers accessing case data?	The data-residency requirement applies not only to the storage and replication of regulated data, but also to remote access to regulated or confidential information by OEMs, subcontractors and support personnel located outside South Africa.
Does Postbank hold Microsoft E5 or the equivalent Defender, Entra ID P2 and Purview licensing, or must the bidder price these? They are not itemised in the pricing schedule.	Postbank already owns Microsoft license
Which cloud environments are actually in production today, at what scale, and who currently holds the tenant/root accounts?	Postbank operates a hybrid environment that includes public-cloud services. Bidders must demonstrate capability across the cloud platforms specified in the RFP. Detailed workload inventory, tenancy and architecture will be provided to the successful bidder during controlled discovery.
For MTTD of 15 minutes, does the clock start at log ingestion into the SIEM, at alert generation, or at the source event timestamp?	For indicative tender sizing, bidders may use a baseline of approximately 100 EPS, with scalable pricing for growth. Exact log-source inventory, peak rates, daily volume, retention tiers and onboarding priorities will be validated with the successful bidder during mobilisation. Bidders must state all sizing and retention assumptions.
Containment SLAs of 15 minutes (privileged account compromise) and 60 minutes (critical incident) are only achievable with delegated authority. Will Postbank grant standing pre-approval for the bidder to isolate endpoints, disable accounts, revoke sessions and block traffic without per-incident approval? If not, will SLA relief apply while awaiting authorisation?	POSTBANK recognises that the specified containment SLAs require appropriately delegated authority and pre-defined response procedures, particularly for high-risk events such as privileged-account compromise and critical security incidents
Many SLAs depend on Postbank or third-party action (change approval, system owner access, OEM support). Will the contract include a dependency and SLA-relief mechanism?	Certain contractual SLAs may depend on actions, approvals or services outside the successful bidder's direct control, including POSTBANK change approvals, system-owner access, third-party service providers, OEM support, network/connectivity availability and other agreed dependencies.
What are the change management windows, freeze periods and CAB lead times, and how do these interact with the 7-day critical patch SLA?	POSTBANK recognises that certain contractual SLAs may depend on actions, approvals or services outside the successful bidder's direct control, including POSTBANK change approvals, system-owner access, third-party service providers, OEM support, network/connectivity availability and other agreed dependencies
The 95% patch compliance and 7-day critical remediation targets imply administrative control over servers and endpoints. Is the bidder expected to execute patching, or to drive and report on remediation performed by Postbank's infrastructure team or another provider?	The bidder is accountable for driving vulnerability and patch remediation to closure within the RFP SLAs, including prioritisation, coordination, tracking, validation and reporting. Where implementation requires action by a Postbank/OEM/application owner, the bidder must coordinate and verify closure. Exceptions must follow Postbank's formal risk-acceptance process. Detailed constrained-system inventories will be shared post-award.
Are there known legacy or end-of-support systems that cannot meet the patching SLA, and how will these be treated?	The bidder is accountable for driving vulnerability and patch remediation to closure within the RFP SLAs, including prioritisation, coordination, tracking, validation and reporting. Where implementation requires action by a Postbank/OEM/application owner, the bidder must coordinate and verify closure. Exceptions must follow Postbank's formal risk-acceptance process. Detailed constrained-system inventories will be shared post-award.
Is the required SOC dedicated (Postbank-exclusive analysts and platform tenancy) or a dedicated service delivered from a shared multi-tenant platform?	The service capability and accountability must be dedicated to Postbank. Shared underlying technology may be proposed only where Postbank data, configurations, access, telemetry and operations are securely segregated and all RFP, PCI DSS and data-residency requirements are met.
Will the bidder's SOC facility be assessed as a TPSP within Postbank's PCI DSS scope and listed on Postbank's AOC? Please confirm the expected responsibility matrix.	The successful SOC bidder will be treated as a Third-Party Service Provider (TPSP) where its services, systems, personnel or processes support or affect Postbank's PCI DSS environment. The final PCI DSS scope and the manner in which the TPSP is referenced in Postbank's PCI DSS documentation, including the applicable AOC, will be determined through the formal PCI DSS scoping and assessment process with Postbank's appointed QSA.The bidder must therefore provide sufficient evidence to support Postbank's PCI DSS compliance and assessment obligations, including applicable policies, procedures, security controls, audit evidence, incident records, access controls, vulnerability management, logging/monitoring and relevant independent assurance reports or certifications
On SOC relocation to Postbank premises: does this cover platform, personnel, or both? Will Postbank provide the facility, and how will licence transferability and residual amortised cost be treated on relocation?	The relocation clause applies to the contracted SOC service capability. Detailed personnel, platform, facility, licence-transfer and commercial arrangements will be agreed with the successful bidder through an approved transition plan and change-control process. Bidders must identify any portability or residual-cost constraints in their proposals.
How many bidder personnel are expected to be resident on Postbank premises under the integrated operating model in Section 10.1?	Postbank has not prescribed a fixed permanently resident headcount. Bidders must propose a staffing model sufficient to meet the 24x7x365 service, SLA, incident-response, knowledge-transfer and integrated-operating-model requirements, including on-site support when required.
For personnel vetting (ITC and criminal clearance): who bears the cost, what is the acceptable validity period, and does it extend to OEM and subcontractor staff?	The successful bidder is responsible for ensuring that all personnel requiring access to Postbank systems, premises or information are appropriately vetted before onboarding, including relevant subcontractor/OEM personnel. Detailed validity and re-screening requirements will follow Postbank policy and applicable law.
Please provide the list of critical services with their target RTO and RPO. The SLA refers to "agreed service-specific recovery windows" but none are stated.	Service-specific criticality, RTO/RPO values and recovery priorities are security-sensitive and will be confirmed with the successful bidder during controlled mobilisation. Bidders must demonstrate capability to support risk-based recovery tiers and the service-specific recovery windows required by Postbank.
Who owns the backup estate today, and what technology is in use? Is the bidder expected to assume operation of it, replace it, or integrate detection and validation on top of it?	Postbank's backup and recovery environment is an existing brownfield capability and is currently operated under Postbank's existing infrastructure and/or appointed service-provider arrangements. The detailed ownership model, technology components, versions, licensing and contractual arrangements will be validated during the requirements-confirmation and mobilisation phase
Immutable/isolated backup capacity is not itemised in the pricing schedule. Should storage capacity and infrastructure be priced, and against which data volumes?	Immutable/ tamper-resistant recovery capability is required. Bidders must provide a transparent scalable pricing model and state storage/ retention assumptions. Final protected volumes, growth, retention and recovery tiers will be validated with the successful bidder during mobilisation

For the clean-room recovery environment: who provides the compute, storage and network capacity, where is it hosted, and what percentage of the production estate must it be sized to restore concurrently?	The bidder must propose an appropriate isolated/ clean recovery capability that meets the RFP's resilience, South African data-residency, security and recovery-validation requirements. Detailed sizing and target recovery scope will be agreed with the successful bidder after validation of critical-service dependencies
Are HSMs currently deployed (payment HSM versus general purpose), what make and model, and is the bidder expected to provide HSM-as-a-service or manage Postbank-owned devices? Does the scope include PCI PIN Security key management, ceremonies and TR-39 style attestation?	Postbank operates a brownfield/ hybrid security environment with existing internal capabilities, security technologies and third-party arrangements. Detailed OEMs, versions, topology, contractual dependencies and control configurations are security-sensitive and will be disclosed to the successful bidder under controlled access during mobilisation. Bidders must propose an interoperable, vendor-neutral approach and clearly identify assumptions
Zero Trust and micro-segmentation (Section 3.3) may require network hardware refresh or a dedicated segmentation platform, neither of which appears in the pricing schedule. Is capital expenditure in scope, and who funds it?	The Zero Trust and micro-segmentation requirements in Section 3.3 are intended to be delivered using the existing Postbank network and security infrastructure where technically feasible. Postbank does not intend for the bidder to assume that a wholesale network hardware refresh or dedicated segmentation platform is automatically required.The bidder must assess the existing environment and propose an appropriate architecture that meets the required Zero Trust, segmentation, access-control and monitoring outcomes
NDR, CSPM/CWPP, TIP, UEBA, WAF, secure web gateway, email gateway and MFA are required in scope but absent from the pricing schedule line items. Should these be added under "Other Operational Services Costs", or will a revised pricing schedule be issued?	The capabilities identified in the clarification - including NDR, CSPM/CWPP, TIP, UEBA, WAF, Secure Web Gateway, Email Gateway and MFA - form part of the required solution scope where applicable and should be priced transparently as distinct solution components.Bidders should not assume that these mandatory capabilities may simply be absorbed into "Other Operational Services Costs" without providing sufficient cost visibility
What is the expected volume of digital forensics work? Is a fixed annual retainer of hours expected in the base price, with overage at agreed rates?	The workload is event-driven and cannot be reliably forecast. Bidders should include a clearly defined base forensic service/ retainer and transparent unit rates for additional specialist effort, with no assumption regarding incident frequency or nature
Who bears cloud consumption and egress charges for log shipping and storage - is the "Cloud Hosting Costs" line intended to cover Postbank's cloud spend or the bidder's platform hosting?	Bidders must clearly separate bidder-hosted platform/ SOC costs from any Postbank-owned cloud consumption assumptions. All bidder-incurred hosting required to deliver the proposed service must be included in the bid unless the pricing schedule expressly states otherwise. Any dependency on Postbank cloud services must be separately identified
Which third-party integrations are in scope for monitoring (SITA, SAPO, BankservAfrica, PASA participants, other), and who owns the connectivity and the right to instrument it?	The service must monitor Postbank-controlled telemetry and, where contractually and technically available, relevant security telemetry from external integrations. Specific third-party names, connectivity architecture and instrumentation rights will be confirmed with the successful bidder during controlled mobilisation
Section 9.6 requires all tooling, detection content and workflows to be exportable and free from restrictive licensing. OEM SIEM, EDR and PAM licences are generally non-transferable. Does Postbank expect licences to be procured in Postbank's name, or is exportability limited to data, configuration and content?	Bidders must identify the proposed licence ownership model and any OEM transfer restrictions. Postbank requires full portability of its data, configurations, rules, workflows and Postbank-specific content at exit. OEM licence transferability will be governed by the applicable OEM terms and the final contract. no undisclosed lock-in is acceptable
Does Postbank expect ownership of bidder-proprietary detection content and playbooks at exit, or a perpetual licence to use Postbank-specific derivatives?	The bidder retains ownership of its pre-existing proprietary IP. Postbank must own, or have a perpetual right to use, all Postbank-specific configurations, detections, playbooks, workflows, documentation and derivatives created for the service, subject to final contractual IP terms
What are the expected format standards for exported detection content (Sigma, STIX/TAXII, vendor-native), and is there an agreed test to demonstrate portability?	Postbank requires export in open, industry-recognised formats where technically feasible, with vendor-native export permitted where no suitable open standard exists. The successful bidder must demonstrate practical portability of Postbank-specific data, detection content, configurations and workflows before exit
Will the demonstration be conducted on the bidder's live production SOC or a lab environment? Will it be on-site or remote, what duration is allocated, and will the ransomware, M365 compromise and recovery-validation scenarios be issued in advance?	The live demonstration will be conducted at the bidder's premises as stated in the RFP. Bidders may use a controlled demonstration environment that credibly demonstrates the required operational capabilities. Logistics, duration and scenario instructions will be issued consistently to qualifying bidders before the demonstration
We respectfully request an extension of the closing date for RFP 04/06/26-27. The additional time will enable us to conduct a thorough review of the requirements, coordinate the necessary technical and commercial inputs, and submit a comprehensive and compliant proposal.	The extension is approved. The revised closing date and time has been communicated through the formal SCM addendum/ notice, which prevails for all bidders
To assist with accurate solution sizing and OEM pricing	
Total number of endpoints in scope, including users, servers, laptops/desktops, ATMs, VMs and cloud workloads.	For tender sizing, use an indicative baseline of up to 1,200 user endpoints and up to 200 servers. VM, cloud-workload and other designated endpoint quantities will be validated during mobilisation. The proposed licensing model must be scalable
SIEM sizing information, including number of log sources, estimated EPS/GB per day and required log retention period.	For indicative tender sizing, bidders may use a baseline of approximately 100 EPS, with scalable pricing for growth. Exact log-source inventory, peak rates, daily volume, retention tiers and onboarding priorities will be validated with the successful bidder during mobilisation. Bidders must state all sizing and retention assumptions
Number of Microsoft 365 users/mailboxes.	The environment uses Microsoft 365. Exact mailbox/ licence populations will be validated during mobilisation. Where pricing depends on mailbox count, bidders must provide transparent scalable/ unit pricing and clearly state the quantity assumptions used
Number of privileged users/accounts and systems requiring PAM.	For pricing, bidders should provide a scalable PAM model and clearly state the assumed quantity bands/ unit rates. Exact privileged-user, service-account, target-system and administrative-account inventories will be validated with the successful bidder during controlled discovery and are not disclosed in the open-bid clarification
Number of assets/IPs requiring vulnerability and patch management.	20
AWS, Azure and GCP workload quantities.	The final quantities of AWS, Azure and GCP workloads will be validated during the mobilisation and discovery phase against the approved cloud inventory
Total data volume requiring backup/cyber recovery and applicable RPO/RTO requirements.	Service-specific criticality, RTO/ RPO values and recovery priorities are security-sensitive and will be confirmed with the successful bidder during controlled mobilisation. Bidders must demonstrate capability to support risk-based recovery tiers and the service-specific recovery windows required by Postbank
Current cybersecurity technologies/platforms already deployed within the Postbank environment.	Postbank currently has a number of cybersecurity technologies and platforms deployed across its environment, including SIEM/ log management, endpoint security, vulnerability management, email security, network security, identity and access management, cloud security, and cryptographic security capabilities
SIEM: number of log sources, EPS/GB per day and required retention period	For indicative tender sizing, bidders may use a baseline of approximately 100 EPS, with scalable pricing for growth. Exact log-source inventory, peak rates, daily volume, retention tiers and onboarding priorities will be validated with the successful bidder during mobilisation. Bidders must state all sizing and retention assumptions
EDR/XDR: number of endpoints, servers, VMs, ATMs and cloud workloads	For tender sizing, use an indicative baseline of up to 1,200 user endpoints and up to 200 servers. VM, cloud-workload and other designated endpoint quantities will be validated during mobilisation. The proposed licensing model must be scalable

PAM: number of privileged accounts/users and systems in scope	For pricing, bidders should provide a scalable PAM model and clearly state the assumed quantity bands/ unit rates. Exact privileged-user, service-account, target-system and administrative-account inventories will be validated with the successful bidder during controlled discovery and are not disclosed in the open-bid clarification
DLP/Microsoft 365: number of users and mailboxes	For tender sizing and pricing, bidders may use an indicative baseline of up to 1,200 users/identities. The final in-scope population will be validated with the successful bidder during mobilisation. Pricing must be scalable and clearly state unit-rate assumptions
Vulnerability and patch management: number of assets/endpoints	200
Cloud environments: AWS, Azure and GCP workload quantities	Postbank operates a hybrid environment that includes public-cloud services. Bidders must demonstrate capability across the cloud platforms specified in the RFP. Detailed workload inventory, tenancy and architecture will be provided to the successful bidder during controlled discovery
Cyber recovery: approximate protected data volume and applicable RPO/RTO requirements	Service-specific criticality, RTO/ RPO values and recovery priorities are security-sensitive and will be confirmed with the successful bidder during controlled mobilisation. Bidders must demonstrate capability to support risk-based recovery tiers and the service-specific recovery windows required by Postbank
Please confirm the number of workstations/laptops, physical servers, virtual machines and cloud workloads that are in scope.	For tender sizing, use an indicative baseline of up to 1,200 user endpoints and up to 200 servers. VM, cloud-workload and other designated endpoint quantities will be validated during mobilisation. The proposed licensing model must be scalable
Please confirm the number of ATMs in scope for the EDR/XDR solution, including the operating system versions currently deployed on the ATMs.	Do not rely on a fixed ATM quantity for base pricing unless specifically stated in the issued pricing schedule/ addendum. The solution must be capable of supporting designated ATM coverage where required. Detailed ATM inventory, platform and version information will be disclosed to the successful bidder under controlled access
3. Please confirm the total number of employees/users in scope for cybersecurity awareness training, as well as the number of active mailboxes and Microsoft 365 users.	For tender sizing and pricing, bidders may use an indicative baseline of up to 1,200 users/identities. The final in-scope population will be validated with the successful bidder during mobilisation. Pricing must be scalable and clearly state unit-rate assumptions
Please confirm Postbank's current Microsoft 365 licensing level, for example E3 or E5, including any existing Microsoft Defender, Microsoft Purview or related security add-ons.	Detailed Microsoft licensing entitlements and enabled security add-ons will be disclosed to the successful bidder during controlled discovery. Bidders must identify all licence dependencies and price any additional licences or add-ons required to meet the RFP rather than assume Postbank will fund unpriced dependencies
For Privileged Access Management (PAM) sizing, please provide the approximate number of:	For pricing, bidders should provide a scalable PAM model and clearly state the assumed quantity bands/ unit rates. Exact privileged-user, service-account, target-system and administrative-account inventories will be validated with the successful bidder during controlled discovery and are not disclosed in the open-bid clarification
- B34Privileged and administrative users	For pricing, bidders should provide a scalable PAM model and clearly state the assumed quantity bands/ unit rates. Exact privileged-user, service-account, target-system and administrative-account inventories will be validated with the successful bidder during controlled discovery and are not disclosed in the open-bid clarification
- Service accounts	For pricing, bidders should provide a scalable PAM model and clearly state the assumed quantity bands/ unit rates. Exact privileged-user, service-account, target-system and administrative-account inventories will be validated with the successful bidder during controlled discovery and are not disclosed in the open-bid clarification
- Target systems/assets that will require PAM integration	Core banking system, AD. 20 servers
For SIEM sizing, please provide the approximate number of log sources and the estimated daily log ingestion volume, preferably in GB per day and/or Events Per Second (EPS).	For indicative tender sizing, bidders may use a baseline of approximately 100 EPS, with scalable pricing for growth. Exact log-source inventory, peak rates, daily volume, retention tiers and onboarding priorities will be validated with the successful bidder during mobilisation. Bidders must state all sizing and retention assumptions
Please confirm the number of sites, networks and network segments that are in scope for network segmentation and/or micro-segmentation.	Detailed network topology, site/ segment inventory and security-zone information will not be disclosed during the open procurement. Bidders must propose a scalable architecture based on the RFP and provide transparent unit/ rate assumptions. The validated topology will be disclosed to the successful bidder during controlled discovery
Please confirm the cloud platforms currently in use, such as Microsoft Azure, AWS and/or Google Cloud Platform, together with the approximate number and type of workloads hosted within these environments.	Postbank operates a hybrid environment that includes public-cloud services. Bidders must demonstrate capability across the cloud platforms specified in the RFP. Detailed workload inventory, tenancy and architecture will be provided to the successful bidder during controlled discovery
With reference to Section 3.12, please clarify which security technologies are currently owned and licensed by Postbank and are expected to be managed by the successful bidder, including technologies such as firewalls, IPS, WAF, email security gateways and related security platforms.	Postbank operates a brownfield/ hybrid security environment with existing internal capabilities, security technologies and third-party arrangements. Detailed OEMs, versions, topology, contractual dependencies and control configurations are security-sensitive and will be disclosed to the successful bidder under controlled access during mobilisation. Bidders must propose an interoperable, vendor-neutral approach and clearly identify assumptions
Please also confirm which technologies the bidder is expected to supply, license and implement as part of the propose	The requirement is governed by the issued RFP. Any detailed current-state information that is not expressly included in the RFP will be provided to the successful bidder during controlled mobilisation where necessary for delivery. Bidders should state all assumptions used for pricing and solution design
Please confirm whether Postbank currently has SIEM, SOAR and/or EDR/XDR platforms in place, and whether these platforms are expected to be:	
- Retained and integrated with	The requirement is governed by the issued RFP. Any detailed current-state information that is not expressly included in the RFP will be provided to the successful bidder during controlled mobilisation where necessary for delivery. Bidders should state all assumptions used for pricing and solution design
- Taken over and managed by the successful bidder	The requirement is governed by the issued RFP. Any detailed current-state information that is not expressly included in the RFP will be provided to the successful bidder during controlled mobilisation where necessary for delivery. Bidders should state all assumptions used for pricing and solution design
- Replaced as part of the proposed solution	The requirement is governed by the issued RFP. Any detailed current-state information that is not expressly included in the RFP will be provided to the successful bidder during controlled mobilisation where necessary for delivery. Bidders should state all assumptions used for pricing and solution design
Please confirm the backup platform or platforms currently in use and whether immutable backup storage is already available, or whether the bidder is required to include immutable storage within the proposed solution and associated pricing.	Postbank operates a brownfield/hybrid security environment with existing internal capabilities, security technologies and third-party arrangements. Detailed OEMs, versions, topology, contractual dependencies and control configurations are security-sensitive and will be disclosed to the successful bidder under controlled access during mobilisation. Bidders must propose an interoperable, vendor-neutral approach and clearly identify assumptions.
For purposes of sizing HSM support services, please confirm the HSM vendor or vendors currently in use and the number of HSM devices that are in scope.	Postbank operates a brownfield/hybrid security environment with existing internal capabilities, security technologies and third-party arrangements. Detailed OEMs, versions, topology, contractual dependencies and control configurations are security-sensitive and will be disclosed to the successful bidder under controlled access during mobilisation. Bidders must propose an interoperable, vendor-neutral approach and clearly identify assumptions.

Section 11.1.2 refers to resources holding CISO and CISSP certifications, while the briefing session referenced CERT. Please confirm the definitive certification requirements applicable to the proposed resources.	The requirement is governed by the issued RFP. Any detailed current-state information that is not expressly included in the RFP will be provided to the successful bidder during controlled mobilisation where necessary for delivery. Bidders should state all assumptions used for pricing and solution design.
Where a proposed technology platform natively provides multiple required capabilities, for example a SIEM platform with integrated SOAR functionality, may bidders provide the combined solution as a single pricing line item, with supporting notes clearly indicating the capabilities included?	The requirement is governed by the issued RFP. Any detailed current-state information that is not expressly included in the RFP will be provided to the successful bidder during controlled mobilisation where necessary for delivery. Bidders should state all assumptions used for pricing and solution design.
Section 3.1 makes provision for the SOC to potentially be relocated to Postbank premises. Should Postbank elect to host the SOC at its own premises, please confirm whether only bidder-facility-related hosting costs would fall away, while software licensing, security tooling, monitoring, SOC resources and managed service costs would remain applicable.	The relocation clause applies to the contracted SOC service capability. Detailed personnel, platform, facility, licence-transfer and commercial arrangements will be agreed with the successful bidder through an approved transition plan and change-control process. Bidders must identify any portability or residual-cost constraints in their proposals.
With regard to penetration testing, Section 3.14 requires penetration testing to be conducted quarterly, while the SLA table indicates a frequency of twice per year. Please confirm the required penetration testing frequency that bidders should use for technical and commercial purposes.	Service-specific criticality, RTO/RPO values and recovery priorities are security-sensitive and will be confirmed with the successful bidder during controlled mobilisation. Bidders must demonstrate capability to support risk-based recovery tiers and the service-specific recovery windows required by Postbank.
penetration testing scope and effort sizing: the approximate number of internal and external IP addresses/hosts in scope, number of web applications and APIs to be tested, and whether ATM, payment and card environments are included in the bidder-delivered testing scope.	Do not rely on a fixed ATM quantity for base pricing unless specifically stated in the issued pricing schedule/addendum. The solution must be capable of supporting designated ATM coverage where required. Detailed ATM inventory, platform and version information will be disclosed to the successful bidder under controlled access.
Does the R20 million Professional Indemnity Insurance requirement need to be held solely by the prime bidder, or may cover from declared delivery partners be considered?	The R20 million Professional Indemnity Insurance requirement must be held by the prime bidder. Where delivery partners or subcontractors are used, their insurance cover may be considered as supplementary, but it does not replace or reduce the prime bidder's obligation to maintain the required R20 million Professional Indemnity Insurance for the contracted services
Must the PCI DSS ROC, ISO 27001 certificate/audit report and POPIA report be in the bidder's name, or will equivalent evidence from declared delivery partners be accepted?	The PCI DSS ROC, ISO/ IEC 27001 certificate/ audit report, and POPIA compliance evidence must be in the prime bidder's name where the requirement relates to the bidder's own organisation, governance, and service delivery capability
Does PCI DSS compliance apply to the SOC facility itself or only to services and environments supporting payment-card data?	PCI DSS compliance applies to the SOC facility and the services it provides to the extent that the SOC stores, processes, transmits, or has security-management access to systems, logs, or information within or supporting Postbank's Cardholder Data Environment (CDE)
Please clarify the required format or recognised assurance standard for the POPIA compliance report.	Postbank does not prescribe a single mandatory format or certification standard for the POPIA compliance report. However, the bidder must provide formal, current, and independently supportable evidence demonstrating compliance with the Protection of Personal Information Act (POPIA) and its applicable regulations
Does the South African hosting requirement apply only to production systems, or also to backups, disaster recovery, telemetry, metadata and platform management services?	All security and service-delivery infrastructure and regulated security telemetry must comply with the South African hosting and data-residency requirements stated in Sections 5.3 and 5.4 of the RFP
Is offshore OEM or specialist support access permitted, provided no regulated Postbank data is stored outside South Africa?	Yes, offshore OEM or specialist support access may be permitted, subject to Postbank's prior written approval and compliance with applicable regulatory, privacy, security, and contractual requirements
Is anonymised telemetry or threat-intelligence data permitted to be processed outside South Africa?	Yes, anonymised telemetry and threat-intelligence data may be processed outside South Africa, subject to Postbank's prior approval and confirmation that the data has been effectively anonymised and cannot reasonably be used to identify Postbank, its customers, users, systems, transactions, or other regulated information
Will a SaaS platform hosted in a South African region satisfy the local-hosting requirement?	All security and service-delivery infrastructure and regulated security telemetry must comply with the South African hosting and data-residency requirements stated in Sections 5.3 and 5.4 of the RFP
When Postbank relocates the SOC, does this refer to the technology platform, the operations team, or the complete SOC capability?	The relocation clause applies to the contracted SOC service capability. Detailed personnel, platform, facility, licence-transfer and commercial arrangements will be agreed with the successful bidder through an approved transition plan and change-control process. Bidders must identify any portability or residual-cost constraints in their proposals
Following SOC relocation, which hosting-related costs are expected to be removed from charges?	The relocation clause applies to the contracted SOC service capability. Detailed personnel, platform, facility, licence-transfer and commercial arrangements will be agreed with the successful bidder through an approved transition plan and change-control process. Bidders must identify any portability or residual-cost constraints in their proposals
Will Postbank provide the infrastructure, connectivity and facilities required for a relocated SOC capability?	The relocation clause applies to the contracted SOC service capability. Detailed personnel, platform, facility, licence-transfer and commercial arrangements will be agreed with the successful bidder through an approved transition plan and change-control process. Bidders must identify any portability or residual-cost constraints in their proposals.
Must all proposed security platforms be deployable within Postbank infrastructure, or may approved South African-hosted SaaS services continue to operate externally?	All security and service-delivery infrastructure and regulated security telemetry must comply with the South African hosting and data-residency requirements stated in Sections 5.3 and 5.4 of the RFP
Please provide current and projected volumes for users, endpoints, servers, ATMs, cloud workloads and privileged accounts required for solution sizing and pricing.	For pricing, bidders should provide a scalable PAM model and clearly state the assumed quantity bands/ unit rates. Exact privileged-user, service-account, target-system and administrative-account inventories will be validated with the successful bidder during controlled discovery and are not disclosed in the open-bid clarification
Please provide current SIEM log volumes, retention requirements and major log sources requiring integration.	For indicative tender sizing, bidders may use a baseline of approximately 100 EPS, with scalable pricing for growth. Exact log-source inventory, peak rates, daily volume, retention tiers and onboarding priorities will be validated with the successful bidder during mobilisation. Bidders must state all sizing and retention assumptions
What security platforms are currently deployed, and which must be retained, integrated, expanded or replaced?	greenfield means Postbank is expecting the bidder to propose and implement the target SOC/ security capability largely as a new environment, rather than simply taking over and maintaining the existing platform
Please provide high-level sizing information for cloud, network and application environments required for pricing and deployment planning.	The proposed SOC capability should be treated as a greenfield target solution, while still providing the necessary integration with Postbank's existing infrastructure, applications, security controls and relevant security platforms
The specification requires quarterly penetration testing, while the SLA requires testing twice annually. Please confirm the required testing frequency.	Bidders must provide penetration testing at least twice per year as the minimum SLA baseline, with additional testing after material changes, significant incidents, regulatory/ audit requirements or where directed by Postbank. The final testing calendar will be agreed during mobilisation
Does "continuous penetration testing" refer to continuous automated validation, recurring manual testing, or both?	Continuous penetration testing" is intended to encompass both continuous automated security validation and recurring manual penetration testing
Is the successful bidder expected to implement remediation directly, or manage and track remediation performed by Postbank teams?	The successful bidder is expected to manage, coordinate and track remediation, while direct remediation will be performed by the responsible Postbank teams or service providers, depending on the affected system and agreed responsibilities
For the live demonstration, will a representative demonstration environment be acceptable, or is a production-equivalent environment required?	A representative demonstration environment is acceptable for the live demonstration. a production-equivalent environment is not mandatory

Must the demonstration include service-delivery processes and operational capabilities in addition to technical functionality?	Yes. The live demonstration must assess both technical functionality and service-delivery/operational capability
What export formats and transition requirements must be supported to satisfy the no-vendor-lock-in requirement?	The successful bidder must support data portability and transition-out in commonly used, non-proprietary and machine-readable formats to prevent vendor lock-in
What baseline quantities should bidders use for the pricing schedule, given that quantity fields and environment volumes are not populated?	As the quantity fields and environment volumes are not populated at tender stage, bidders should not assume unlimited quantities or introduce their own unsubstantiated volumes as the contractual baseline
May bidders provide consumption-based pricing and unit rates for growth in users, endpoints, storage, log ingestion and professional services?	For indicative tender sizing, bidders may use a baseline of approximately 100 EPS, with scalable pricing for growth. Exact log-source inventory, peak rates, daily volume, retention tiers and onboarding priorities will be validated with the successful bidder during mobilisation. Bidders must state all sizing and retention assumptions
Will Postbank issue an updated pricing schedule containing the applicable baseline quantities for pricing purposes?	Service-specific criticality, RTO/ RPO values and recovery priorities are security-sensitive and will be confirmed with the successful bidder during controlled mobilisation. Bidders must demonstrate capability to support risk-based recovery tiers and the service-specific recovery windows required by Postbank
CSIEM Sizing sheet	The requirement is governed by the issued RFP. Any detailed current-state information that is not expressly included in the RFP will be provided to the successful bidder during controlled mobilisation where necessary for delivery. Bidders should state all assumptions used for pricing and solution design
Sites	The requirement is governed by the issued RFP. Any detailed current-state information that is not expressly included in the RFP will be provided to the successful bidder during controlled mobilisation where necessary for delivery. Bidders should state all assumptions used for pricing and solution design
Number of sites	Detailed network topology, site/ segment inventory and security-zone information will not be disclosed during the open procurement. Bidders must propose a scalable architecture based on the RFP and provide transparent unit/rate assumptions. The validated topology will be disclosed to the successful bidder during controlled discovery
	Vendor/Version
Anti-Virus	EDR/XDR
Database	oracle and SQL
Email	365
Proxy	Sophos
Vulnerability Scanner	top 4 on the quadrant
Web servers	Windows and unix
Any other	The requirement is governed by the issued RFP. Any detailed current-state information that is not expressly included in the RFP will be provided to the successful bidder during controlled mobilisation where necessary for delivery. Bidders should state all assumptions used for pricing and solution design
	Vendor/Version
Workstation	windows 11 pro
Servers	linux and windows
Domain Controller	windows
Virtualisation	Vsphere
	Vendor/Version
Storage Devices	one drive
File servers	sharepoint
	Vendor/Version
External firewall	Fortiy products
Internal Firewall	Fortiy products
IDS/IPS	The requirement is governed by the issued RFP. Any detailed current-state information that is not expressly included in the RFP will be provided to the successful bidder during controlled mobilisation where necessary for delivery. Bidders should state all assumptions used for pricing and solution design
Load balancer	F5
VPN appliance	Fortiy products
Router	Cisco
Switch	Cisco
Please confirm the final bid submission deadline and explain what the 3 September 2026 at 16:30 date on the cover represents.	The formal closing date and time are those stated in the latest SCM-issued bid notice/ addendum. Any earlier administrative date shown elsewhere should not be relied on where it conflicts with the formal closing notice
Can Postbank provide a complete inventory of the existing security technologies, licences and service providers?	Postbank operates a brownfield/ hybrid security environment with existing internal capabilities, security technologies and third-party arrangements. Detailed OEMs, versions, topology, contractual dependencies and control configurations are security-sensitive and will be disclosed to the successful bidder under controlled access during mobilisation. Bidders must propose an interoperable, vendor-neutral approach and clearly identify assumptions
Which technologies must the successful bidder take over, and which must be newly supplied, replaced or expanded?	We expect greenfield solution
Please provide the number of users, identities, service accounts and privileged accounts in scope.	For tender sizing and pricing, bidders may use an indicative baseline of up to 1,200 users/ identities. The final in-scope population will be validated with the successful bidder during mobilisation. Pricing must be scalable and clearly state unit-rate assumptions
Please provide the number of laptops, desktops, servers, virtual machines, ATMs and cloud workloads in scope.	Do not rely on a fixed ATM quantity for base pricing unless specifically stated in the issued pricing schedule/ addendum. The solution must be capable of supporting designated ATM coverage where required. Detailed ATM inventory, platform and version information will be disclosed to the successful bidder under controlled access
What are the current average and peak SIEM event rates, measured in events per second?	For indicative tender sizing, bidders may use a baseline of approximately 100 EPS, with scalable pricing for growth. Exact log-source inventory, peak rates, daily volume, retention tiers and onboarding priorities will be validated with the successful bidder during mobilisation. Bidders must state all sizing and retention assumptions
What is the current daily log-ingestion volume, and what searchable and archive retention periods are required?	For indicative tender sizing, bidders may use a baseline of approximately 100 EPS, with scalable pricing for growth. Exact log-source inventory, peak rates, daily volume, retention tiers and onboarding priorities will be validated with the successful bidder during mobilisation. Bidders must state all sizing and retention assumptions
How many log sources and integrations must be onboarded into the SIEM and SOC?	For indicative tender sizing, bidders may use a baseline of approximately 100 EPS, with scalable pricing for growth. Exact log-source inventory, peak rates, daily volume, retention tiers and onboarding priorities will be validated with the successful bidder during mobilisation. Bidders must state all sizing and retention assumptions

How many applications, APIs, databases, internet-facing services, branches, data centres and network devices are in scope?	Detailed network topology, site/ segment inventory and security-zone information will not be disclosed during the open procurement. Bidders must propose a scalable architecture based on the RFP and provide transparent unit/rate assumptions. The validated topology will be disclosed to the successful bidder during controlled discovery
Which systems are classified as critical or crown-jewel services, and what are their recovery time and recovery point objectives?	Service-specific criticality, RTO/ RPO values and recovery priorities are security-sensitive and will be confirmed with the successful bidder during controlled mobilisation. Bidders must demonstrate capability to support risk-based recovery tiers and the service-specific recovery windows required by Postbank
Does Postbank already have immutable backups and an isolated clean recovery environment, or must the bidder supply these?	Postbank will not disclose detailed control-state, maturity gaps or defensive configuration information during the open-bid clarification. Bidders should assume a brownfield environment and propose discovery, integration and uplift activities consistent with the RFP. Detailed current-state information will be provided to the successful bidder under controlled access
Which services require dedicated resources, and which may be delivered through a shared SOC?	The service capability and accountability must be dedicated to Postbank. Shared underlying technology may be proposed only where Postbank data, configurations, access, telemetry and operations are securely segregated and all RFP, PCI DSS and data-residency requirements are met
What minimum on-site presence and South African staffing levels are required?	all staff must be in South africa
Is the bidder responsible for physically implementing patches and remediation, or only for identifying, coordinating and tracking them?	The bidder is accountable for driving vulnerability and patch remediation to closure within the RFP SLAs, including prioritisation, coordination, tracking, validation and reporting. Where implementation requires action by a Postbank/ OEM/ application owner, the bidder must coordinate and verify closure. Exceptions must follow Postbank's formal risk-acceptance process. Detailed constrained-system inventories will be shared post-award
Who may authorize containment actions such as endpoint isolation, account suspension and network blocking?	Containment actions must follow Postbank's approved incident-response authority matrix and change/ security procedures. The bidder must support rapid automated or analyst-led containment within SLA, but disruptive actions must be executed within the delegated authority agreed during mobilisation, including pre-authorised emergency actions
Can consortium members and subcontractors satisfy mandatory requirements using their certifications, personnel and references?	Bidders may participate through a consortium, joint venture, partnership or subcontracting arrangement where permitted by the RFP and applicable SCM requirements. The bid must clearly identify the prime/ accountable party and demonstrate compliance with all mandatory procurement and technical requirements
Is Phase 2 evaluated at 70 points overall, or must the bidder achieve 70 points separately in both Parts A and B?	The RFP states that bidders must achieve the minimum threshold separately for Part A and Part B of Phase 2. The issued RFP/ addendum governs and bidders should respond accordingly
Is penetration testing required quarterly or twice annually?	Bidders must provide penetration testing at least twice per year as the minimum SLA baseline, with additional testing after material changes, significant incidents, regulatory/ audit requirements or where directed by Postbank. The final testing calendar will be agreed during mobilisation
What SLA penalties, service credits and maximum liability will apply?	The applicable service-credit, penalty and liability provisions will be governed by the final SCM-issued contract terms. Bidders should not assume any limitation or remedy that is not expressly stated in those terms
What performance-security amount will be required?	Any performance-security requirement will be as stated in the formal SCM bid/ contract documentation. Where no amount is stated, bidders should not introduce an assumption and should await the formal SCM clarification/addendum
Will annual price adjustments be allowed for labour, licence, cloud and exchange-rate increases?	Pricing must comply with the commercial terms issued by SCM. Bidders should submit the required three-year pricing and clearly disclose any proposed escalation assumptions. no escalation or foreign-exchange adjustment should be assumed unless expressly permitted in the final bid/ contract terms
Are licence quantities fixed, committed minimums or adjustable according to actual consumption?	Quantities stated for tender purposes are baseline sizing assumptions unless expressly identified as committed minima. Bidders must provide scalable/ unit pricing for changes in consumption. Any commercial adjustment during the contract will be subject to the agreed contract and approved change-control process
Does South African data residency permit global cloud control planes and international vendor support, provided the data remains in South Africa?	Any proposed architecture must comply with the RFP's South African hosting and data-residency requirements. No regulated Postbank logs, telemetry or protected data may be stored or replicated outside South Africa. Any offshore control-plane processing, metadata flow or support access must be fully disclosed and is subject to Postbank legal, security and regulatory approval
What Postbank personnel, access, connectivity and change approvals will be available during the first three months?	During the first three months, Postbank will provide the successful bidder with reasonable access to the relevant business, IT, cybersecurity, infrastructure, application and service-management personnel required to support discovery, onboarding, integration, testing and mobilisation
Does the Month 1 deployment period begin at contract signature, purchase order, kickoff or the date on which access is provided?	The mobilisation/deployment clock will commence from the contractual commencement date stated in the final agreement/ appointment documentation, subject to Postbank making agreed prerequisites reasonably available. Detailed dependencies and milestone acceptance will be baselined at kickoff
How many employees, contractors and third-party users are in scope?	Postbank's indicative user population is approximately 1,200 for tender sizing purposes. The validated population, including applicable employee, contractor and third-party-user breakdowns, will be confirmed with the successful bidder during mobilisation. Bidders should state the population included in their base price and provide scalable unit rates for material volume changes.
How many endpoints are in scope, split between laptops, desktops, servers, virtual machines, ATMs and other devices?	For tender sizing, bidders may use an indicative endpoint population of approximately 1,200 user endpoints and approximately 200 server-class workloads. Detailed device-type, ATM, virtual-machine, cloud-workload and other endpoint breakdowns will be validated with the successful bidder during mobilisation. Bidders must state their sizing assumptions and unit rates for additional assets.
How many physical and virtual servers are in scope, split by operating system and environment?	For tender sizing, bidders may use an indicative baseline of approximately 200 server-class workloads. Detailed physical/virtual, operating-system and environment breakdowns are security-sensitive and will be provided to the successful bidder during controlled discovery and mobilisation. Bidders must price a scalable solution and state material assumptions.
How many ATMs are in scope, and what operating systems and network architecture do they use?	Detailed ATM fleet size, operating-system information and network architecture will not be disclosed during the open tender stage. Where ATM security coverage is relevant to the proposed solution, bidders should state their assumptions and provide scalable unit pricing. Validated details will be provided to the successful bidder during mobilisation.
How many identities, service accounts and privileged accounts are in scope?	Detailed identity, service-account and privileged-account populations are security-sensitive and will not be disclosed during the open tender stage. Bidders should propose a scalable PAM/IGA/ITDR model, state the quantities included in their base price and provide unit rates for incremental users/accounts/systems. Final validated volumes will be confirmed with the successful bidder during mobilisation.

How many Microsoft 365 users, mailboxes, Teams users, SharePoint sites and OneDrive accounts are in scope?	For tender sizing, bidders may use an indicative Microsoft 365 user/mailbox population broadly aligned to the approximately 1,200-user enterprise baseline. Detailed Teams, SharePoint, OneDrive and mailbox inventories will be validated with the successful bidder during mobilisation. Bidders should state included quantities and unit rates.
What are the average and peak SIEM event rates in events per second?	For tender sizing, bidders may assume an indicative SIEM ingestion baseline of approximately 100 EPS. Detailed average/peak event profiles, source-by-source volumes and architecture are security-sensitive and will be validated with the successful bidder during mobilisation. Bidders must state included EPS/ingestion assumptions and scalable pricing.
What is the current daily log-ingestion volume in GB or TB?	Detailed current log-ingestion volumes will not be disclosed during the open tender stage. Bidders should derive their storage assumptions from the indicative SIEM sizing baseline and required retention, clearly state those assumptions, and provide scalable pricing for additional ingestion/storage. Validated volumes will be confirmed during mobilisation.
What searchable and archive retention periods are required for each log type?	Bidders should provide for a baseline security/audit-log retention model that supports applicable legal, regulatory, PCI DSS and Postbank requirements. Detailed retention by log type and any differentiated searchable/archive requirements will be confirmed with the successful bidder during detailed design and mobilisation.
How many log sources and integrations must be onboarded?	Postbank does not prescribe a fixed number of log sources and integrations at tender stage. The successful bidder will receive the validated inventory during mobilisation. Bidders should price a scalable onboarding model and state the number/type of integrations included in their base price and unit rates for additional sources.
Please provide the log-source breakdown by firewalls, servers, endpoints, databases, applications, cloud services, identity platforms and banking systems.	At tender stage, bidders should assume that relevant security telemetry may need to be integrated from standard enterprise categories such as network/security controls, servers/endpoints, identity, databases, applications and cloud services. Detailed source inventories, products, versions and banking-system integration details are security-sensitive and will be provided to the successful bidder during controlled mobilisation.
How many applications, APIs, databases and internet-facing services are in scope?	Postbank does not prescribe fixed quantities for applications, APIs, databases or internet-facing services at tender stage. Bidders should state the quantities included in their base price and provide scalable unit rates. Validated inventories will be confirmed with the successful bidder during mobilisation.
How many AWS, Azure and GCP accounts, subscriptions, projects and workloads are in scope?	Postbank uses cloud services as part of its technology environment; detailed account, subscription, project and workload quantities will not be disclosed during the open tender stage. Bidders should propose a scalable cloud-security pricing model, state included quantities and provide unit rates. Validated details will be confirmed during mobilisation.
How many locations, data centres, branches, network devices and security zones are in scope?	Detailed location, data-centre, branch, network-device and security-zone inventories are security-sensitive and will not be disclosed during the open tender stage. Bidders should state their sizing assumptions and provide scalable unit pricing. Validated infrastructure/network inventories will be provided to the successful bidder during controlled mobilisation.
How many security devices must be managed, split by vendor, product, model and version?	Detailed security-device inventories by vendor, product, model and version are security-sensitive and will not be disclosed during the open tender stage. Bidders should demonstrate vendor-agnostic integration capability, state any assumptions and identify unit pricing or commercial impacts for additional managed devices. Validated inventories will be provided during mobilisation.
What are the current monthly volumes for alerts, incidents, service requests, changes and forensic investigations?	Detailed historical alert, incident, service-request, change and forensic-investigation volumes will not be disclosed during the open tender stage. Bidders should size the managed service to meet the required SLAs, state operational workload assumptions and identify how pricing scales if volumes materially change. Validated baselines will be confirmed during mobilisation.
How many vulnerabilities are identified monthly, and what is the current remediation backlog?	Detailed vulnerability volumes and remediation backlog information are security-sensitive and will not be disclosed during the open tender stage. Bidders should price the required vulnerability-management service against the indicative environment sizing, state workload assumptions and provide scalable pricing. Validated data will be shared with the successful bidder during mobilisation.
How many employees require annual training, and how frequently must phishing simulations be performed?	For tender sizing, bidders may use the indicative enterprise user baseline for security-awareness licensing. Final eligible populations and the detailed phishing-simulation programme will be confirmed with the successful bidder during mobilisation. Bidders should state included user quantities, campaign assumptions and unit rates for changes.
Please provide a complete inventory of incumbent security platforms and licences.	Postbank will provide a validated inventory of incumbent security platforms, licences, quantities/capacity, expiry dates, support arrangements and service providers during the controlled procurement/mobilisation process.
Which platforms must be retained, expanded, replaced or newly deployed?	Postbank does not prescribe that all incumbent platforms must be retained. Bidders must assess the existing environment and clearly identify which platforms they propose to retain, integrate, expand, replace or newly deploy, including the commercial and technical rationale and any migration costs
Which existing licences are owned by Postbank, and when do they expire?	The validated licence schedule will identify Postbank-owned, provider-owned and subscription-based licences, together with applicable expiry/renewal dates. Bidders must distinguish existing licences from new licences required for the proposed service.
Are the current licences transferable to the appointed service provider?	Licence transferability is dependent on the applicable vendor licensing terms and ownership arrangements. Bidders must identify which incumbent licences can be transferred, assigned or utilised by the appointed service provider and identify any restrictions or additional costs
Are bidders free to propose their preferred technology stack?	Yes. Bidders may propose their preferred technology stack, provided that it meets all mandatory functional, technical, security, regulatory, service-level and integration requirements. Bidders must clearly identify any proposed replacement of incumbent technologies and associated transition costs
Are there mandatory or preferred vendors?	No specific vendor should be assumed to be mandatory unless expressly stated elsewhere in the tender. Solutions must support interoperability with Postbank's existing environment and avoid unnecessary vendor lock-in.
Will Postbank accept bidder-owned, multi-tenant platforms if all data remains in South Africa?	Yes, subject to compliance with Postbank's security, data-residency, POPIA, PCI DSS, regulatory, contractual and architectural requirements. The bidder must clearly disclose the hosting location, data-processing locations, control plane, support locations, subcontractors and any cross-border access or processing.
Must all technology become Postbank-owned, or may it remain a managed-service platform?	Technology does not necessarily have to become Postbank-owned. Bidder-owned or managed-service platforms may be proposed where permitted by the tender requirements. The bidder must clearly state ownership, licensing, subscription, renewal and exit arrangements and ensure that Postbank can retrieve its data, configurations, rules, logs and other required artefacts at contract termination.

Which current vendors and service providers must participate in transition?	The incumbent service providers and relevant technology owners will participate in transition where required and subject to contractual arrangements. Bidders must identify all dependencies and transition activities requiring incumbent participation and include them in the mobilisation plan.
Will the incumbent provider supply configurations, rules, playbooks, documentation and historical data?	Postbank will require reasonable cooperation from incumbent providers to support an orderly transition, subject to contractual rights, security controls and availability of the relevant information. This may include configurations, integration information, rules/use cases, playbooks, documentation, asset inventories, historical security data and other operational artefacts required for continuity. Bidders must clearly identify any information or dependencies they require from incumbents
Which systems are classified as crown-jewel or critical services?	Postbank will provide the validated list of critical/crown-jewel services and supporting systems during mobilisation. Classification will be based on business criticality, customer impact, regulatory requirements, data sensitivity, operational dependencies and approved BIA/BCP/DR requirements
What are the recovery time and recovery point objectives for each critical service?	RTO and RPO values will be determined from Postbank's approved BIA/BCP/DR requirements and validated during mobilisation. Bidders must demonstrate how their proposed solution can meet the applicable RTO/RPO for each critical service and clearly identify any assumptions or dependencies.
What total data volume must be protected by immutable or isolated backups?	The final protected data volume will be validated from the current infrastructure, application and backup inventories during mobilisation. Bidders must state the storage capacity included in their proposal, retention assumptions, compression/deduplication assumptions, growth allowance and unit pricing for additional capacity
What backup platforms are currently used?	Postbank will provide the current backup-platform inventory during mobilisation. Bidders may propose integration with existing platforms or replacement where technically and commercially justified. Any proposed replacement must include migration, licensing, implementation and exit implications.
Does Postbank already have an isolated recovery environment or clean room?	The availability and capability of the existing isolated recovery/clean-recovery environment will be validated during mobilisation. Bidders must identify whether their solution requires a dedicated clean room, isolated recovery environment or can utilise existing Postbank/cloud infrastructure, and must separately price any additional infrastructure required.
How many applications must be included in quarterly and annual recovery exercises?	The final application list will be based on Postbank's approved critical-service and DR scope. Bidders must provide capacity to support the agreed recovery-exercise programme and state any assumptions regarding the number of applications, systems, databases and workloads included.
Must the clean recovery environment remain permanently available or be activated on demand?	The recovery model may be persistent, standby or on-demand, depending on the criticality and RTO/RPO of the applicable service. Bidders must state the proposed recovery model for each service tier and clearly identify the cost and recovery-time implications of on-demand activation.
Who is responsible for application, database and business-data validation after recovery?	The bidder will be responsible for supporting and validating the technical recovery of the contracted infrastructure/security components. Application owners, database owners and business owners remain responsible for functional and business-data validation and acceptance. Responsibilities must be clearly documented in the RACI matrix.
Are production-sized recovery resources required, or may reduced-capacity resources be used?	Recovery capacity must be aligned with the approved RTO/RPO, criticality and business requirements. Reduced-capacity resources may be proposed where they can demonstrably meet the applicable recovery objectives. Bidders must clearly state the recovery capacity, assumptions, scaling mechanism and expected performance during recovery.
Which services require dedicated personnel, and which may be delivered from a shared SOC?	Dedicated/named resources should cover Postbank service management, security governance, reporting, major-incident coordination, threat hunting, compliance/audit support and key technical escalation. Core 24x7 SOC monitoring, alert triage, correlation, threat intelligence and SOAR activities may be delivered from a shared SOC, provided Postbank receives dedicated accountability and the required SLAs. Bidders must clearly identify dedicated versus shared FTEs.
Is a minimum on-site team required?	Yes. Postbank requires an appropriate South African-based on-site capability for governance, operational engagement, major incidents, workshops, audits and other activities requiring physical presence. Bidders must propose the minimum on-site staffing model and identify when additional on-site resources will be required.
What SOC analyst volumes, shift coverage and escalation structure does Postbank expect?	
Must all personnel be based in South Africa?	The SOC must operate 24x7x365. Bidders must propose an appropriate L1/L2/L3 staffing and escalation model capable of meeting the required incident SLAs. The bidder must state analyst capacity per shift, supervisory coverage, escalation paths, after-hours support and surge capacity during major incidents.
How long does personnel vetting normally take?	Core SOC operations and key customer-facing/security governance resources must be South Africa-based, particularly where access to Postbank systems or sensitive information is required. Any offshore personnel, if proposed and permitted, must be explicitly identified together with their location, role, access, data-processing implications and applicable security controls.
Which activities remain Postbank's responsibility?	Personnel vetting requirements and timelines will be confirmed during mobilisation. Bidders must submit personnel information early enough to support Postbank's access and vetting processes and must include vetting as a dependency in their mobilisation plan. No personnel may receive production access before completing the applicable Postbank security, access and vetting requirements.
Is the bidder responsible for physically deploying patches, or only identifying and tracking remediation?	Postbank retains responsibility for security governance and risk acceptance, business/application ownership, approval of high-impact changes and containment actions where authorisation is required, infrastructure/application remediation unless explicitly included in the contract, access approvals, change management and final business acceptance. The bidder is responsible for contracted SOC monitoring, investigation, escalation, reporting, coordination and remediation tracking.
Who approves containment actions such as isolating endpoints, disabling accounts or blocking network traffic?	The bidder is primarily responsible for identifying, prioritising, coordinating and tracking remediation. Physical patching or configuration changes remain with Postbank or the relevant technology/service owner unless explicitly included in the bidder's contracted scope. Any changes performed by the bidder must follow Postbank's change-management, access-control and security procedures.
Does Postbank require named, dedicated forensic, cloud, IAM, PAM, application-security and compliance specialists?	

What are the expected service desk hours, channels, languages and ticketing integrations?	Containment must follow Postbank's approved incident-response governance and playbooks. The bidder may automatically execute pre-approved, low-risk containment actions where explicitly authorised. High-impact or potentially disruptive actions require approval from an authorised Postbank security representative, unless an approved emergency playbook expressly permits autonomous execution. The bidder must maintain a complete audit trail.
From what point is the 15-minute detection-to-containment SLA measured?	The line item will be discussed during contracting and SLA phases
Does the 15-minute SLA pause while awaiting Postbank approval?	The line item will be discussed during contracting and SLA phases
Are SLA penalties applicable, and what is the penalty structure or service-credit cap?	The line item will be discussed during contracting and SLA phases
Is penetration testing required quarterly or twice annually?	The line item will be discussed during contracting and SLA phases
Does the seven-day critical vulnerability SLA apply to findings outside the bidder's control?	The line item will be discussed during contracting and SLA phases
What Postbank resources will be available during the first three months?	The line item will be discussed during contracting and SLA phases
Will Postbank guarantee timely access, change approvals, network connectivity and application owners?	The line item will be discussed during contracting and SLA phases
Does Month 1 mean 30 calendar days after contract signature, purchase order or access being granted?	The line item will be discussed during contracting and SLA phases
Can the deployment timetable be adjusted where incumbent licences or integrations cause delays?	The line item will be discussed during contracting and SLA phases
Does South African data residency apply only to customer data and telemetry, or also to metadata, support logs and backups?	South African data-residency requirements apply to Postbank data processed or stored as part of the service, including security telemetry/logs, customer or sensitive data, relevant metadata, backups and service/support data where it contains Postbank information. Bidders must clearly identify where each category of data is stored, processed, backed up and accessed. Any cross-border transfer or processing must be explicitly disclosed and must comply with Postbank's security, regulatory, contractual and POPIA requirements.
Are global cloud control planes permitted if data storage remains in South Africa?	Potentially, subject to Postbank's approval and security requirements. Bidders must disclose the location of the control plane, management plane, telemetry/metadata, support systems and subprocessors. A bidder must demonstrate that use of a global control plane does not result in unauthorised cross-border storage, processing or access to Postbank information.
May international vendor support personnel access the environment?	International support access is not automatically permitted. Any proposed offshore access must be explicitly disclosed, justified and approved by Postbank before access is granted. Access must be subject to least privilege, MFA, privileged-access controls, session logging, time-bound access and Postbank's applicable security and regulatory requirements.
Does Postbank require two geographically separated South African hosting locations?	The proposed SOC/security platform must provide appropriate resilience and disaster-recovery capability within South Africa. Bidders should propose two geographically separated South African locations or an equivalent architecture capable of meeting the required availability, continuity and recovery objectives. The bidder must state the locations, architecture, RTO/RPO and associated costs.
What connectivity will Postbank provide between its environment and the bidder's SOC?	Postbank will provide or facilitate the required connectivity subject to its network architecture, security controls and change-management processes. Bidders must specify their connectivity requirements, bandwidth, protocols, IP requirements, encryption, collector architecture and redundancy requirements. Connectivity must be designed to avoid a single point of failure.
Who pays for connectivity, circuits and redundancy?	Bidders must include all connectivity, circuits, bandwidth, collectors, redundancy and associated recurring costs required to deliver their proposed service, unless the tender explicitly identifies a Postbank-provided service. Any Postbank-provided connectivity must be clearly identified as an assumption in the bidder's commercial proposal.
What budget or estimated contract value has been approved?	Confidential
Is the intended evaluation definitely 90/10?	Yes
What does the cover-page date of 3 September 2026 at 16:30 represent?	Closing date for submission of clarification question/enquires
Is Phase 2 evaluated at 70 points overall or 70 points separately for Parts A and B?	already answered
What performance-security amount will apply?	already answered
Are subcontractors and consortium members permitted to satisfy mandatory technical requirements?	already answered
Can partner certifications, references and personnel be used for Phase 1 and Phase 2 scoring?	already answered
How is the requirement to hold three listed certifications interpreted, given that CISSP, CEH and OSCP are individual certifications?	already answered
Must the PCI DSS ROC relate to the bidder's own environment, or may a partner or hosted platform provide it?	already answered
What level of Professional Indemnity Insurance evidence must be submitted with the bid?	already answered
What are the email submission size, format, encryption and attachment requirements?	already answered
Will pricing adjustments be allowed during the three-year term for licence, cloud and salary increases?	already answered
Are licence volumes fixed, committed minimums or adjustable according to actual consumption?	Not fixed
Mandatory eligibility	Yes. Bidders must submit evidence demonstrating compliance with all mandatory Phase 1 requirements, whether met directly or through an arrangement expressly permitted by the RFP. Evaluation will be conducted strictly against the published requirements.
Sizing confidence	Postbank has provided sufficient indicative information for tender-stage pricing. Bidders must clearly state their sizing assumptions, quantities included in base pricing and scalable unit rates. Security-sensitive and final validated volumes will be provided to the successful bidder during mobilisation and detailed design.
Technology model	Bidders may propose technology that meets the published functional, security, regulatory, integration and service requirements. Postbank is not prescribing a specific technology stack unless expressly stated in the RFP. Any proposed retention, replacement or introduction of technology must be clearly justified, costed and supported by a transition approach.
Delivery feasibility	Bidders must demonstrate that the Month 1 to Month 3 commitments are achievable and identify all assumptions, dependencies, required Postbank inputs and critical-path activities in their mobilisation plan. Access and dependencies will be managed through the agreed governance and implementation process with the successful bidder.
SLA exposure	Bidders must assess the published SLA requirements, measurement points, dependencies, exclusions and contractual remedies and incorporate the associated delivery and commercial risk into their proposals. Any clarification or qualification must be explicitly stated in the bid and will remain subject to the RFP and final contractual terms.

Data residency	Yes. Proposed technology, hosting, support and operating models must comply with the South African data-residency, privacy, security, regulatory and contractual requirements stated in the RFP. Any cross-border processing, support access, control-plane dependency or subprocessor arrangement must be explicitly disclosed for Postbank review.
Commercial viability	The bidder's three-year price must be complete for the proposed solution and include all costs necessary to deliver the contracted scope, including licences/subscriptions, infrastructure/hosting, implementation, transition, operations, support, labour and other identified dependencies, subject to the commercial terms of the RFP. Bidders must clearly disclose assumptions, exclusions and any permitted price-adjustment mechanisms.

Technology or Managed Service	Postbank Response	Required	Our Capability	Delivery Model	Category
24/7 Security Operations Centre	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Partner	Operations
SIEM and log management	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Partner	Operations
SOAR and automated response	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Hybrid	Operations
EDR/XDR for endpoints, servers and ATMs	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Hybrid	Endpoint
Threat intelligence platform	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Hybrid	Operations
Threat hunting	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Hybrid	Operations
Incident response and digital forensics	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Hybrid	Operations
Multi-Factor Authentication	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Hybrid	Identity
Identity Governance and Administration	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Hybrid	Identity
Single Sign-On	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Internal	Identity
Identity threat detection	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Internal	Identity
Privileged Access Management	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Internal	Identity
User behaviour and insider-threat monitoring	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Internal	Identity
Network detection and response	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Hybrid	Network
Firewalls, IPS and secure web gateways	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Hybrid	Network
Network segmentation and Zero Trust	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Hybrid	Network
Web Application Firewall and DDoS protection	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Partner	Network
Email security and anti-phishing	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Partner	Email
Microsoft 365 security	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Hybrid	Email
Data Loss Prevention	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Hybrid	Data
Cloud security for Azure, AWS and GCP	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Partner	Cloud
Application and API security testing	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Hybrid	Application
Vulnerability scanning and management	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Hybrid	Vulnerability
Patch management	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Partner	Vulnerability
Penetration testing and attack simulation	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Partner	Testing
Encryption and Hardware Security Modules	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Internal	Data
Immutable backup and clean cyber recovery	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Internal	Recovery
Security awareness and phishing simulations	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Partner	People
Compliance, risk and audit reporting	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Internal	Governance
Security device management	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Internal	Operations
South African hosting and data residency	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Internal	Hosting

Implementation and system integration	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Internal	Delivery
Training and knowledge transfer	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Partner	Delivery
Transition-in and transition-out services	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Internal	Delivery
Monthly and executive security reporting	Bidder to confirm capability, delivery model and evidence against the RFP requirement. No additional Postbank current-state security detail is required at this stage	Yes	Yes	Partner	Reporting
Number of users	For tender sizing and pricing, bidders may use an indicative baseline of up to 1,200 users/identities. The final in-scope population will be validated with the successful bidder during mobilisation. Pricing must be scalable and clearly state unit-rate assumptions.	1200			
Number of endpoints/workstations	For tender sizing, use an indicative baseline of up to 1,200 user endpoints and up to 200 servers. VM, cloud-workload and other designated endpoint quantities will be validated during mobilisation. The proposed licensing model must be scalable.	1200			
Number of servers	For tender sizing, use an indicative baseline of up to 200 servers. The final server/VM population will be validated during mobilisation and the bidder must provide scalable unit pricing.	200			
Number of mailboxes	The environment uses Microsoft 365. Exact mailbox/licence populations will be validated during mobilisation. Where pricing depends on mailbox count, bidders must provide transparent scalable/unit pricing and clearly state the quantity assumptions used.	1500			
List of operating systems in use (including versions)	The environment includes multiple supported operating-system families. Detailed OS/version inventories are security-sensitive and will be disclosed to the successful bidder during controlled discovery. Bidders must demonstrate support for heterogeneous enterprise endpoint/server environments.	windows and linux			
Number of privileged accounts requiring management	For pricing, bidders should provide a scalable PAM model and clearly state the assumed quantity bands/unit rates. Exact privileged-user, service-account, target-system and administrative-account inventories will be validated with the successful bidder during controlled discovery and are not disclosed in the open-bid clarification.	20			
Does Postbank use VMWare or Hypervisor	Yes. Refer to the RFP and any formal SCM addendum for the governing requirement.	yes			
Please complete sizing questionnaire	The requirement is governed by the issued RFP. Any detailed current-state information that is not expressly included in the RFP will be provided to the successful bidder during controlled mobilisation where necessary for delivery. Bidders should state all assumptions used for pricing and solution design.				
Include additional technologies necessary to meet the mandatory technical requirements, or	additional technology are welcomed	additional technology are welcomed			
Restrict their proposal to the technologies explicitly listed in the Pricing Schedule.	The requirement is governed by the issued RFP. Any detailed current-state information that is not expressly included in the RFP will be provided to the successful bidder during controlled mobilisation where necessary for delivery. Bidders should state all assumptions used for pricing and solution design.				
How many DEVICES (servers, network devices) do you want to manage for Privileged Accounts?	*For pricing, bidders should provide a scalable PAM model and clearly state the assumed quantity bands/unit rates. Exact privileged-user, service-account, target-system and administrative-account inventories will be validated with the successful bidder during controlled discovery and are not disclosed in the open-bid clarification*				
How many DEVICES (servers, network devices) do you want to change passwords of managed Privileged Accounts (Password Management)?	*For pricing, bidders should provide a scalable PAM model and clearly state the assumed quantity bands/unit rates. Exact privileged-user, service-account, target-system and administrative-account inventories will be validated with the successful bidder during controlled discovery and are not disclosed in the open-bid clarification*				
How many DEVICES (servers, network devices) do you want to manage for SESSION RECORDING?	*Detailed network topology, site/ segment inventory and security-zone information will not be disclosed during the open procurement. Bidders must propose a scalable architecture based on the RFP and provide transparent unit/ rate assumptions. The validated topology will be disclosed to the successful bidder during controlled discovery*				
How many PAM Users do you need to manage?	*For pricing, bidders should provide a scalable PAM model and clearly state the assumed quantity bands/ unit rates. Exact privileged-user, service-account, target-system and administrative-account inventories will be validated with the successful bidder during controlled discovery and are not disclosed in the open-bid clarification*				
Where are the PAM Users defined (i.e. Active Directory)? PAM will authenticate the Users verifying their Password (MS Domain password or locally defined on PAM)	*For pricing, bidders should provide a scalable PAM model and clearly state the assumed quantity bands/ unit rates. Exact privileged-user, service-account, target-system and administrative-account inventories will be validated with the successful bidder during controlled discovery and are not disclosed in the open-bid clarification*				
How many Symantec PAM NODES (Active-Active) do you need for PRODUCTION environment?	*For pricing, bidders should provide a scalable PAM model and clearly state the assumed quantity bands/ unit rates. Exact privileged-user, service-account, target-system and administrative-account inventories will be validated with the successful bidder during controlled discovery and are not disclosed in the open-bid clarification*				
How many Symantec PAM NODES do you need for DISASTER RECOVERY environment?	*For pricing, bidders should provide a scalable PAM model and clearly state the assumed quantity bands/ unit rates. Exact privileged-user, service-account, target-system and administrative-account inventories will be validated with the successful bidder during controlled discovery and are not disclosed in the open-bid clarification*				
How many Symantec PAM NODES do you need for DEVELOPMENT environment?	*For pricing, bidders should provide a scalable PAM model and clearly state the assumed quantity bands/ unit rates. Exact privileged-user, service-account, target-system and administrative-account inventories will be validated with the successful bidder during controlled discovery and are not disclosed in the open-bid clarification*				
How many concurrent user sessions do you want to have to the Symantec PAM server?	*For pricing, bidders should provide a scalable PAM model and clearly state the assumed quantity bands/ unit rates. Exact privileged-user, service-account, target-system and administrative-account inventories will be validated with the successful bidder during controlled discovery and are not disclosed in the open-bid clarification*				
How many STUDENTS do you want to register for the CA PAM Admin Training?	*For pricing, bidders should provide a scalable PAM model and clearly state the assumed quantity bands/ unit rates. Exact privileged-user, service-account, target-system and administrative-account inventories will be validated with the successful bidder during controlled discovery and are not disclosed in the open-bid clarification*				
Symantec PAM comes in 3 appliance formats: **- VMWare OVA (virtual)** **- Amazon AWS AMI (Private Cloud)** **- MS Azure VHD (Private Cloud)** **Which format would you prefer?**	*Bidders should propose the PAM architecture, capacity and HA/ DR model required to meet the RFP availability, resilience, data-residency and security requirements. Detailed existing topology and sizing will be provided to the successful bidder during controlled discovery*				

DEVICE Name, Type and Version	**Number of DEVICES of this type**	**Password Management (Y/N)**	**How do you access this DEVICE?** **E.g. SSH, Remote Desktop, Web Browser, SQLPLUS, etc**

Microsoft Windows Server 2012	*15*	*Y*	*Detailed device types, versions, access methods and inventory quantities are security-sensitive and will be provided to the successful bidder during controlled discovery. Bidders should provide scalable PAM pricing and identify supported integration methods*
RedHat Enterprise Linux 6.6	*20*	*Y*	*Detailed device types, versions, access methods and inventory quantities are security-sensitive and will be provided to the successful bidder during controlled discovery. Bidders should provide scalable PAM pricing and identify supported integration methods*
CISCO Router 5500	*30*	*N*	*Detailed device types, versions, access methods and inventory quantities are security-sensitive and will be provided to the successful bidder during controlled discovery. Bidders should provide scalable PAM pricing and identify supported integration methods*
Oracle Database 11g	*30*	*N*	*Detailed device types, versions, access methods and inventory quantities are security-sensitive and will be provided to the successful bidder during controlled discovery. Bidders should provide scalable PAM pricing and identify supported integration methods*