



BID NUMBER	ECIC05P-2026/27
NAME OF BID	ECIC05P-2026/27: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS
QUESTIONS AND ANSWERS	

The following questions were received by the Export Credit Insurance Corporation of South Africa (SOC) Limited (ECIC) on the abovementioned bid, and are hereby responded to as follows:

Number	Question	Reference	Response
1.	Good Day, Please may you kindly confirm if an equivalent solution, accreditations and experience will be accepted for Microsoft Solutions Partner Status and COBIT 2019 certified resource. Kind Regards,		ECIC ICT Governance Framework is based on COBIT and GCICPFT; the assessor must be COBIT 2019 Design and Implementation certified. A certified Microsoft partner is indispensable, as ECIC operates mainly in the Microsoft™ environment.
2.	Good day Ms Makwela With reference to Bid ECIC05P-2026/27 – Cybersecurity Managed Services and Licences for a Period of Three Years, Could you kindly assist us with the following clarification questions: 2.1. With reference to paragraph 3.3, can ECIC provide a more detailed inventory of the in-scope environment, including the number and operating systems of servers, number of endpoints, laptops/workstations, network devices, cloud workloads and remote-user devices?	Paragraph 3.3	The OS on all servers is Windows; the list includes the environments the ECIC has including core tools and OS. Explicit listing/mention of 5 Windows servers (and factored the possibility of the servers growing with 2 additional servers in the future in the same Windows environment), 120 users, 6 switches and 5 Wifi Access points. NOTE: Please see the pricing template as a guide that requested the quoting for 180 endpoints for vulnerability management.



BID NUMBER	ECIC05P-2026/27
NAME OF BID	ECIC05P-2026/27: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS
QUESTIONS AND ANSWERS	

Number	Question	Reference	Response
	2.2. With reference to paragraph 5.1.4, does ECIC require the proposed vulnerability-management solution to perform actual automated patch deployment/remediation, or is vulnerability identification, prioritisation and remediation guidance sufficient?	Paragraph 5.1.4	Both (currently patching is done using Kaspersky, which does not cater for network devices amongst other assets). See 'G' of 5.1.4: “In addition to the products and services highlighted above, the bidder must have the capacity to assist the ECIC in reactive and proactive support. ”
	2.3. Does ECIC permit the deployment of lightweight agents on endpoints and servers for vulnerability assessment, or must the proposed solution primarily use agentless network-based scanning?		ECIC does not have servers on premises. Servers are hosted in a private cloud externally. ECIC is not prescriptive on agent or agentless scanning as long as: • The is no expectation for the ECIC to provide a server infrastructure. • The solution accommodates for remote working and on premise. • Full details on the agents and security controls for it are made available to the ECIC.
	And for remote users, are devices continuously connected to the corporate network/VPN, or should vulnerability assessment operate independently while users are outside the ECIC network?		The vulnerability assessment must operate independently while users are outside of the ECIC network. Users do not continuously connect to the ECIC network when they are offsite.



BID NUMBER	ECIC05P-2026/27
NAME OF BID	ECIC05P-2026/27: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS
QUESTIONS AND ANSWERS	

Number	Question	Reference	Response
	2.4. Can ECIC confirm the expected number of assets/endpoints to be licensed for vulnerability management, including servers, workstations/laptops, network devices and remote-user devices?		180 Endpoints as full scope (Current plus factoring growth).
	2.5. Can ECIC confirm the exact Kaspersky product/version, current licensing model, number of licensed endpoints and whether the existing Kaspersky management console is cloud-hosted or on-premises? And Will ECIC provide the successful bidder with administrative/read-only access to the Kaspersky management platform for monitoring, health checks and configuration recommendations?		• Cloud-hosted version. • The successful bidder will be given access to assist the ECIC with second-line support and may be required to log calls with Kaspersky™ on behalf of the ECIC. • Please refer to managed services 5.1.4; g (bidder to provide proactive and reactive support; this translates the administrative role attached to the task).
	2.6. Can ECIC confirm the number of protected workloads currently covered by N-able Cove, including servers, endpoints and any Microsoft 365 workloads?		ECIC has its own N-Able™ licenses which it may decide to review with the successful bidder or any provider in line with its procurement processes. Current N-Able™ license count (160 – including dormant accounts). ECIC to adjust annually during the license's renewal, which is managed separately from this RFP.



BID NUMBER	ECIC05P-2026/27
NAME OF BID	ECIC05P-2026/27: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS
QUESTIONS AND ANSWERS	

Number	Question	Reference	Response
	And is the successful bidder expected to perform backup restores/testing directly, or only monitor backup health and provide recommendations?		The successful bidder will work with the ECIC resources during backup testing. Generally, the ECIC resources will inform the service provider what to restore. The restore is done live (on the call), and evidence is recorded. Both are required.
2.7.	Can ECIC confirm whether all approximately 100–120 users are licensed with Microsoft 365 E3 and whether there are any additional Microsoft security licences currently deployed, such as Defender for Office 365, Defender for Endpoint, Entra ID P1/P2 or Intune?		The ECIC environment is growing. At the time of publishing this RFP, the license count was a total of 120 including licenses used for service accounts. However, the end users were about 100. The total license count is being increased to 130. End users are expected to be close to 120.
	And is the successful bidder expected to perform configuration changes directly, or provide recommendations and have ECIC's internal security personnel implement the changes?		Both. The bidder is expected to augment ECIC capacity and skill. The ECIC has one Security resource and one infrastructure management resource. The work is therefore shared/escalated to the service provider.
2.8.	With reference to paragraph 5.1.1.2, which CIS Benchmarks does ECIC expect to be assessed and implemented for Microsoft 365 and the hosted Windows Server environment, Does ECIC require a formal CIS Benchmark assessment report showing the current score, identified gaps and remediation status?	Paragraph 5.1.1.2	Currently, the M365™ environment is assessed against CIS benchmarks (using a tool) and a report is issued as part of the monthly SLA report.



BID NUMBER	ECIC05P-2026/27
NAME OF BID	ECIC05P-2026/27: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS
QUESTIONS AND ANSWERS	

Number	Question	Reference	Response
	And is the bidder expected to implement the recommended CIS configuration changes, or provide recommendations for ECIC approval and implementation?		Yes, together with the ECIC resources. Recommendations are prioritised and pre-approved.
2.9.	DMARC		DNS hosted externally.
	2.9.1. Can ECIC confirm the current DNS/email architecture for ecic.co.za, including the email service provider and whether SPF and DKIM are currently implemented?		Exchange online. Mimecast email security (Inbound and Outbound). Outbound emails go via Rocketseed™ for automated email signatures. SPF and DKIM are implemented.
	And Does ECIC expect the proposed DMARC solution to provide monitoring only, or should the bidder also configure and progressively implement the DMARC policy from monitoring through enforcement?		The bidder is expected to implement together with the ECIC resources.
2.10.	Knowb4		Current License count for Knowbe4 110, the License count is subject to change as and where there are new users.
	2.10.1. Can ECIC confirm the current KnowBe4 licence edition, number of licensed users and whether the successful bidder will be expected to administer the existing KnowBe4 tenant?		The bidder must assist the ECIC to co-manage its cybersecurity awareness platform.



BID NUMBER	ECIC05P-2026/27
NAME OF BID	ECIC05P-2026/27: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS
QUESTIONS AND ANSWERS	

Number	Question	Reference	Response
			The following are expected from the bidder: - Provide two annual interactive sessions, one for staff and the other for Management, and the sessions can either be online/ in person. The staff session is to be arranged as a Cyber Day in person. - Provide Phishing simulations leading up to each of the interactive sessions. -Increase ECIC internal capacity by providing guidance, platform administration and campaign management. - Assist with strategic advisory based on insights from the KnowBe4 platform and monthly reporting to ensure effective and measurable cyber-awareness training.
	2.10.2. For the quarterly phishing simulations, does ECIC expect the bidder to design campaigns, configure campaigns, analyse results and provide remediation recommendations, or only provide advisory services based on existing KnowBe4 reports?		The bidder must assist the ECIC to co-manage its cybersecurity awareness platform, this includes planning, scheduling and rolling out phishing campaigns, the reports are generated by the system, however the monthly report must translate high levels and possible improvements/opportunities to improve the awareness training of the employees of ECIC



BID NUMBER	ECIC05P-2026/27
NAME OF BID	ECIC05P-2026/27: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS
QUESTIONS AND ANSWERS	

Number	Question	Reference	Response
	2.11. Cybersecurity awareness — onsite requirements 2.11.1. Can ECIC confirm the expected number of participants and preferred location(s) for the two annual in-person cybersecurity awareness sessions?		Head Office (Centurion) 100 to 120 people.
	2.11.2. With reference to paragraphs 5.1.7 and 5.1.8, can ECIC provide the most recent ISO 27001:2022 and COBIT 2019 assessment reports, including identified findings, current maturity/capability levels and outstanding remediation actions?	Paragraphs 5.1.7 and 5.1.8	To be provided to the successful bidder.
	2.11.3. Can ECIC confirm whether the required ISO 27001:2022 engagement is a gap/readiness assessment and follow-up assessment, or whether ECIC expects the appointed service provider to support the organisation through formal ISO 27001 certification?		No formal ISO certification is needed. ECIC need a follow-up assessment. The last assessment was conducted in December 2024.
	2.11.4. For the COBIT 2019 assessment, does ECIC expect assessment against all COBIT 2019 governance and management objectives, or will ECIC provide the specific objectives/processes that should be assessed?		The last assessment focused on all governance and management objectives, at an activity level. The follow-up may be expected to cover the same.



BID NUMBER	ECIC05P-2026/27
NAME OF BID	ECIC05P-2026/27: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS
QUESTIONS AND ANSWERS	

Number	Question	Reference	Response
	2.11.5. Can ECIC confirm the dates of the previous ISO 27001 and COBIT 2019 assessments and whether the successful bidder will be required to use the previous assessment findings as the baseline for the new assessment?		ISO27001- December 2024. COBIT 2019 – January to March 2025.
	2.11.6. Can ECIC clarify whether the 16 hours per month are intended to cover the actual execution of all weekly health checks and reporting activities, or whether they are primarily allocated to reporting/advisory activities with technical remediation performed from the separate support-hours allocation?		Mainly towards weekly health checks and reporting for in-scope items. The 16 hours are the maximum number of hours expected to be used for reporting and health checks. It is anticipated that some bidders may utilise tools for this portion of work, which may utilise less than 16 hours monthly. Any remediation that ECIC needs assistance with will mainly be covered under the 260 annual support hours.
	2.11.7. Can ECIC confirm whether the 260 annual support hours may be used for implementation and remediation arising from the monthly health checks, ISO/COBIT assessments, vulnerability remediation, M365 remediation and other in-scope services?		Yes, as and when pre-approved by the ECIC.
	2.11.8. Does ECIC have specific requirements regarding the geographic location of security, vulnerability, DMARC and backup-management data, including		SA or jurisdictions that have privacy laws equivalent to SA laws/GDPR.



BID NUMBER	ECIC05P-2026/27
NAME OF BID	ECIC05P-2026/27: CYBERSECURITY MANAGED SERVICES AND LICENSES FOR A PERIOD OF THREE YEARS
QUESTIONS AND ANSWERS	

Number	Question	Reference	Response
	requirements for data to remain within South Africa?		
	2.11.9. With reference to the various managed cybersecurity services and technologies specified under Section 5.1, can ECIC confirm whether the successful bidder will be required to integrate the in-scope security platforms, including Microsoft 365, Kaspersky EDR, vulnerability management, N-able Cove, DMARC and KnowBe4, with an existing ECIC SIEM/SOC platform?	Section 5.1	SIEM / SOC integration will be required. This is a separate procurement process.
	If integration is required, please provide details of the existing SIEM platform and confirm which data sources/logs are expected to be onboarded and monitored.		N/A at this stage.