

REQUEST FOR BIDS

BID DETAILS

BID NUMBER:		FB-SETA (25-26) T0001
CLOSING	Date:	30 June 2025
	Time:	12:00 pm
DESCRIPTION:		The appointment of a cyber security service provider for a period of three (3) years.
TECHNICAL QUERIES EMAIL ADDRESS:		scm@foodbev.co.za
CONTACT:		011 253 7300
LOCATION:		7 Wessel Road Rivonia, 2128
BRIEFING SESSION:		No briefing session
Validity Period		120 Days

DETAILS OF BIDDER

Organisation/individual: _____

Contact person: _____

Telephone/ Cell number: _____

E-mail address: _____

GLOSSARY

AWARD	Conclusion of the procurement process and final notification to the effect to the successful bidder
B-BBEE	Broad-based Black Economic Empowerment in terms of the Broad-based Black Economic Empowerment Act, 2003 (Act No. 53 of 2003) and the Codes of Good Practice issued thereunder by the Department of Trade and Industry
BID	Written offer in a prescribed or stipulated form in response to an invitation by FOODBEV SETA for the provision of goods, works or services
CONTRACTOR	Organisation with whom FOODBEV SETA will conclude a contract and potential service level agreement subsequent to the final award of the contract based on this Request for Bid
CORE TEAM	The core team are those members who fill the non-administrative positions against which the experience will be measured.
DUE DILIGENCE	A verification of information that has been received during application to assess the applicant's operational capacity.
FOODBEV SETA ("FBS")	Food and Beverage Manufacturing Sector Education and Training Authority
ORIGINAL BID	Original document signed in ink, or copy of original document signed in ink,
ORIGINALLY CERTIFIED	To comply with the principle of originally certified, a document must be both stamped and signed in original ink by a commissioner of oaths.
SCHEDULE 3A ENTITY	As per the classification by the National Treasury these refer to other National public entities
SCM	Supply Chain Management
SLA	Service Level Agreement

TABLE OF CONTENTS

GLOSSARY	2
SECTION A	4
1. INTRODUCTION	4
2. BACKGROUND	4
3. PURPOSE	4
4. SCOPE OF WORK	5
5. DELIVERABLES	6
6. REPORTING AND COMMUNICATION	7
7. METHODOLOGY AND APPROACH	7
8. REQUIRED RESOURCES	7
9. KEY PERFORMANCE INDICATORS (KPIs)	7
10. DURATION OF ENGAGEMENT	7
11. PRICING SCHEDULE	8
12. VALIDITY PERIOD	10
SECTION B	10
13. BID EVALUATION PROCESS	10
SECTION C	16
14. TENDER SUBMISSION INSTRUCTIONS	16
15. AUTHORISATION	18
16. ANNEXURES	19

**INVITATION TO BID FOR THE APPOINTMENT OF A CYBER SECURITY SERVICE PROVIDER
FOR A PERIOD OF THREE (3) YEARS.**

SECTION A

1. INTRODUCTION

The Food and Beverages Manufacturing SETA ("FoodBev SETA") is a Schedule 3A Public Entity established in terms of the Skills Development Act 97 of 1998. FoodBev SETA is currently operating in Johannesburg at Number 7 Wessel Road, Rivonia Sandton. FoodBev SETA's function is to promote, facilitate and incentivize skills development in the Food and Beverages Manufacturing Sector. FoodBev SETA is one of the 21 Sector Education and Training Authorities (SETAs) across the economy mandated to implement the National Skills Development Plan (NSDP) outcomes.

2. BACKGROUND

FoodBev SETA, following a comprehensive Cybersecurity Assessment conducted by a service provider, is committed to enhancing its cybersecurity posture. The assessment benchmarked FoodBev SETA's information security technology architecture against the Centre for Internet Security (CIS) version 8.0 standard and identified critical gaps and opportunities for improvement.

This document outlines the Terms of Reference for a service provider to implement and refine specific cybersecurity controls and recommendations identified in the assessment report, as prioritised by FoodBev SETA's ICT management and to provide overall cyber security services.

3. PURPOSE

The primary purpose of engaging a cybersecurity service provider is to:

- 3.1 Implement and refine critical cybersecurity controls within FoodBev SETA's IT infrastructure and networks (perimeter, network, endpoints, applications, and data layers).
- 3.2 Address specific key areas of concern identified in the assessment, namely: Data Protection, Application Security improvements, Audit Log management, Threat and Vulnerability management, and formalised Penetration Testing.
- 3.3 Improve the "As Is State (currently at 64%)" maturity across the targeted cybersecurity layers towards the defined target maturity of 93%, as benchmarked against the CIS Controls version 8.0 and aligned with the NIST Cybersecurity Framework (NST-CSF).
- 3.4 Cyber security operations and monitoring.
- 3.5 Provide cyber security services that include improvement of governance, compliance, develop policies and procedures, and risk management.
- 3.6 Ensure continuous cybersecurity monitoring, risk mitigation, and proactive threat management to maintain a robust security posture beyond maturing benchmarks.

4. SCOPE OF WORK

The service provider will be responsible for the implementation and operationalization of cybersecurity controls in the following key areas:

4.1 Data Protection

Objective: To establish comprehensive data protection capabilities beyond current native encryption and planned initiatives, focusing on the discovery, classification, monitoring, and robust protection of sensitive data.

Specific Tasks:

- 4.1.1 Implement a solution to monitor access, use, and distribution of data, whether at Rest, In Motion, or In Use.
- 4.1.2 Establish a data protection program, complemented by data leakage and loss prevention (DLP) capabilities.
- 4.1.3 Implement controls to encrypt data on removable media.
- 4.1.4 Implement controls to encrypt sensitive data in transit or at rest.
- 4.1.5 Improve controls for securely disposing of data.

4.2 Application Security

Objective: To implement processes and templates for managing security vulnerabilities and hardening configurations for commercially used applications within FoodBev SETA's environment, addressing the current exposure on the Application Layer.

Specific Tasks:

- 4.2.1 Establish and implement a process for root cause analysis on security vulnerabilities identified in applications
- 4.2.2 Establish and implement a severity rating system and process for application vulnerabilities
- 4.2.3 Develop and implement standard hardening configuration templates for application infrastructure

4.3 Audit Log Management

Objective: To implement centralised log collection, correlation, and security event alerting to enhance detection capabilities for indicators of compromise.

Specific Tasks:

- 4.3.1 Implement a solution for centralised audit log collection.
- 4.3.2 Implement a solution for centralised security event alerting
- 4.3.3 Establish and Implement processes for audit log review and correlation

4.4 Threat and Vulnerability management

Objective: To perform periodic internal and external penetration tests and ensure proper remediation of identified findings. To proactively assess risk and threats to our environment.

Specific Tasks:

- 4.4.1 Perform periodic vulnerability scanning and penetration testing (internal and external assets).
- 4.4.2 Proactive risk assessment, threat intelligence, and mitigation strategies.
- 4.4.3 Develop and oversee a process for the remediation of penetration test findings.

4.5 Security operations and Monitoring

- 4.5.1 24/7 security operations center (SOC) services for real time threat detection
- 4.5.2 Incidence response and forensic investigation capabilities
- 4.5.3 Define and adhere to incident responses SLA's
- 4.5.4 Conduct bi-annual incident response.

4.6 Additional services

- 4.6.1 Provide advice on future initiatives, potential acquisitions and evolving cyber security threats
- 4.6.2 Provide strategic guidance on cyber governance, policies and risk management ensuring compliance with POPIA, GDPR (if applicable), and other relevant regulations.
- 4.6.3 Conduct annual re-assessment using the CIS controls and NST-CSF framework to measure ongoing maturity improvements and identify new gaps

4.7 Continuous Cybersecurity Assurance

Objective: To ensure that cybersecurity measures remain effective against evolving threats, with regular reviews, updates, and proactive threat hunting.

Specific tasks:

- 4.7.1 Conduct periodic threat assessments and adjust controls as needed
- 4.7.2 Provide real-time security advisories on emerging threats
- 4.7.3 Ensure all implemented controls remain effective through validation exercise (eg red teaming)

5. DELIVERABLES

The successful bidder must provide measurable outcomes, including but not limited to:

- 5.1 A detailed Implementation Plan for each scoped area.
- 5.2 Documented processes and procedures for all newly implemented or refined controls (e.g., Data Classification Scheme, Application Vulnerability Management Process, Audit Log Management Process, Penetration Testing Program).
- 5.3 Deployment, configuration, and integration of relevant cybersecurity solutions (e.g., Data Protection/DLP solution, centralised logging and alerting tools).
- 5.4 Reports on the findings and remediation status of all conducted periodic internal and external penetration tests.
- 5.5 Regular progress reports detailing achievements against the "To Be State" target maturity of 93% for the relevant controls
- 5.6 Knowledge transfer sessions and, where applicable, training to FoodBev SETA staff to ensure sustainability of the implemented controls.
- 5.7 Recommendations for future initiatives and necessary acquisitions where current capabilities are insufficient or new threats emerge
- 5.8 A compliance report detailing alignment with POPIA and other relevant regulatory frameworks.
- 5.9 A detailed exit strategy, including knowledge transfer sessions, documentation, and transitions

support for internal teams or a new vendor.

6. REPORTING AND COMMUNICATION

The service provider must establish a clear reporting structure, providing regular updates (e.g., weekly, bi-weekly, monthly) to FoodBev SETA's ICT Manager and relevant stakeholders as indicated by FoodBev SETA. Communication shall be transparent, highlighting progress, challenges, and proposed solutions. All documentation and reports should be clear, concise, and actionable.

7. METHODOLOGY AND APPROACH

The service provider shall adopt an implementation methodology that aligns with and leverages the principles of the CIS Critical Security Controls (CIS Controls) version 8.0 standard and the NIST Cybersecurity Framework (NST-CSF) categories (Identify, Detect, Protect, Respond, Recover). The approach should focus on pragmatic implementation of controls to achieve the target maturity levels, demonstrating a defense-in-depth set of best practices. The approach must not be generic or artificially intelligent created, it must be specific to FBS demonstrating understanding and knowledge. The service provider must ensure that the solutions proposed are based on open standards, avoiding proprietary lock-in where possible, and must provide documentation for seamless future transitions.

8. REQUIRED RESOURCES

The proposed team members should possess a strong foundational understanding of cybersecurity best practices, defense-in-depth principles, and demonstrate familiarity with the CIS Critical Security Controls (version 8.0) and the NIST Cybersecurity Framework. Experience working within complex IT environments that integrate solutions from various vendors.

9. KEY PERFORMANCE INDICATORS (KPIs)

Progress will be rigorously measured against the target "To Be State" maturity of 93% for the specific controls identified within the scope of work. Detailed KPIs will be mutually agreed upon based on the approved implementation plan but will include, at minimum:

- 9.1 Percentage improvement in maturity levels for Data Protection, Application Security (scoped areas), Audit Log Management (scoped areas), and Penetration Testing controls
- 9.2 Timely completion of project phases and deliverables according to the agreed-upon timeline.
- 9.3 Effectiveness of implemented solutions in meeting defined security objectives (e.g., accurate data classification, identified and remediated application vulnerabilities, effective incident detection via centralized alerting).
- 9.4 Mean time to detect (MTTD) and mean time to respond (MTTR) to security incidents.
- 9.5 The number of critical vulnerabilities remediated within agreed SLA timelines.
- 9.6 Reduction in incidents due to implemented controls (e.g. phishing malware, unauthorised access)

10. DURATION OF ENGAGEMENT

This engagement will be for a period of three (3) years.

10.1 Pricing Schedule

#	Task	Deliverables (ToR Reference)	Solution Approach (Brief Description)	Resource Allocation (Roles/Hours)	Year 1	Year 2	Year 3	Total Cost
1.	Data Protection	DLP solution, encryption controls, data classification scheme	E.g., "Deploy Symantec DLP with 3-tier classification"	e.g.1 Architect, 2 Engineers (200 hrs)	R	R	R	R
2.	Application Security	Vulnerability management process, hardening templates			R	R	R	R
3.	Audit Log Management	SIEM deployment, alerting rules, correlation processes			R	R	R	R
4.	Threat & Vulnerability Management	Penetration tests (internal/external), remediation oversight			R	R	R	R
5.	SOC & Monitoring	24/7 SOC, incident response, forensics			R	R	R	R
6.	Additional Services	Annual reassessment, strategic advisory, development of policies and procedures, governance and compliance			R	R	R	R
7.	Continuous cyber security assurance	Threat assessments, red teaming, advisories			R	R	R	R
8.	Project Management & Governance	Implementation plans, stakeholder reports, presentation at committees			R	R	R	R
	Sub Total				R	R	R	R
	VAT				R	R	R	R

#	Task	Deliverables (ToR Reference)	Solution Approach (Brief Description)	Resource Allocation (Roles/Hours)	Year 1	Year 2	Year 3	Total Cost
	TOTAL				R	R	R	R

10.2 Mandatory Pricing Requirements

Bidders must provide:

- a. Hourly/Daily Rates (if applicable) for key roles
- b. License/Tool Costs (e.g., "SIEM license: R 250,000/year").
- c. Escalation Clause

Submission Format

Bidders must submit pricing in:

- a. Excel (with formulas for totals).
- b. PDF (signed by authorised representative).

Pricing Structure

- a. Contract Duration: 3 years.
- b. Currency: All costs in R (incl. VAT).
- c. Escalation: Specify annual escalation rate (if applicable).

11. VALIDITY PERIOD

The Bidder is required to confirm that it will hold its proposal valid for 120 days from the closing date of the submission of proposals, during which time it will maintain without changing the personnel proposed for the services together with their proposed rates.

SECTION B

12. BID EVALUATION PROCESS

12.1 The Bid evaluation process will be undertaken in accordance with the following staged approach:

Stage 1:	Administrative requirements
Stage 2:	Functionality Criteria
Stage 3:	The Preferential Procurement Policy Framework Regulation using the 80:20 points system.

12.2 Stage 1: Administrative Requirements

Stage	Criteria	Requirements
Stage 1	Administrative requirements	<p>The potential bidder must submit three (3) copies of the bid proposal as follows: i) Two (2) hard copies</p> <p>(a) One (1) electronic copy in PDF format saved on a USB memory stick</p> <p>Requirements for Hard Copies:</p> <p>(b) The bid proposal must be securely bound, hole-punched, and sequentially numbered in accordance with the response format outlined in Section C of this bid document.</p> <p>Requirements for Electronic Copy:</p> <p>(c) The electronic copy must be saved in PDF format on a USB memory stick.</p> <p>(d) The files must be organized into clearly labelled, paginated, and indexed folders in accordance with the response format outlined in Section C of this bid document.</p> <p>Standard bidding documents:</p> <p>(e) Submission of fully completed and duly signed SBD forms (declarations must be answered truthfully to the best of bidder's knowledge).</p> <p>(f) A valid tax clearance certificate or confirmation of pin.</p> <p>(g) A valid B-BBEE certificate or affidavit</p> <p>Foreign Qualifications:</p> <p>(h) <i>Bidders must ensure that foreign qualifications are accompanied by SAQA evaluation. Foreign qualifications not accompanied by the SAQA evaluation will not be evaluated and will be disqualified.</i></p> <p>Important Note: FBS will not be responsible for any misinterpretation or misplaced information resulting from a proposal that is not properly labelled, paginated, and indexed</p>

12.3 Stage 2: Functionality Evaluation Criteria

1. DETAILED FUNCTIONALITY EVALUATION CRITERIA:		WEIGHTING ALLOCATED
1.1 Project Team		
<p>This illustrates the minimum expected resources to be utilised in the project as indicated in number 8 above. The bidder must provide an organogram for the team members in the project with a comprehensive CV for each project member, qualifications and certifications.</p> <p>Important notes for bidders:</p> <ol style="list-style-type: none"> 1) Please note that points will only be awarded if the bidder submits both the CV demonstrating relevant experience, relevant qualifications and all required certifications. If CVs, qualification and certification are not submitted, no points will be allocated. 2) Foreign qualifications must be accompanied by SAQA evaluation. If foreign qualifications are not accompanied by the SAQA evaluation, no points will be allocated. 3) The certification/s must be valid at the time of bid submission. 		
1.1.1 Project Lead: Cybersecurity Manager		15.00
<p>Experience:</p> <p>At least 5 years of experience in leading cybersecurity implementation projects, with a strong focus on strategic planning, project management, and stakeholder engagement. Proven track record in successfully delivering complex cybersecurity initiatives, preferably involving CIS Controls and/or NIST Cybersecurity Framework implementation.</p> <p>Minimum Requirements:</p> <ol style="list-style-type: none"> 1) NQF level 7 qualification 2) Certification in Project Management Professional Certification (PMP) or PRINCE2 (Practitioner) or Certified Scrum Master (CSM) or PMI-ACP (Agile Certified Practitioner) 3) An abridged CV indicating a minimum of 5 years' experience in leading cybersecurity implementation projects, with a strong focus on strategic planning, project management, and stakeholder engagement. 		
CV submitted demonstrating 5 or more years' experience in leading cybersecurity implementation projects, qualifications (NQFL 7) and a certification		15.00
CV submitted demonstrating a minimum of 3 years but less than 5 years' experience in leading cybersecurity implementation projects, qualification (NQFL 7) and a certification		10.00
CV submitted demonstrating a minimum of less than 3 years' experience in leading cybersecurity implementation projects, qualifications (NQFL 7) and a certification		0.00

1. DETAILED FUNCTIONALITY EVALUATION CRITERIA:	WEIGHTING ALLOCATED	
No CVS, qualification and certification submitted	0.00	
1.1.2 Security Operation Center (SOC) lead Experience: At least 5 years' experience in a Security Operations Center (SOC) environment including incident response, threat hunting, security monitoring, and vulnerability management. Minimum Requirements: 1) NQF 7 in Computer Science, Cyber Security or Information and Communication Technology related qualification or equivalent. 2) Certified in Security+ and Certified Ethical Hacker (CEH) or CompTIA CySA+ and Certified Ethical Hacker (CEH) 3) An abridged CV indicating a minimum of 5 years' in technical and management experience in SOC and/or in the field.		15.00
	15.00	
	10.00	
	0.00	
	0.00	

1. DETAILED FUNCTIONALITY EVALUATION CRITERIA:	WEIGHTING ALLOCATED	
1.1.3 Cyber Security Architect/ Engineer Experience: At least 5 years of hands-on experience in designing, implementing, integrating, and configuring cybersecurity solutions in enterprise environments. The architect must demonstrate expertise in: <ol style="list-style-type: none"> 1) Data Loss Prevention (DLP) technologies, data classification methodologies, data discovery tools, and data lifecycle management. 2) Application vulnerability management processes, secure coding principles (for guidance and review), hardening best practices, and familiarity with secure software development lifecycles. 3) Deploying, configuring, and managing Security Information and Event Management (SIEM) solutions, centralised log collection platforms, log correlation techniques, and security event alerting mechanisms. Minimum Requirements: <ol style="list-style-type: none"> 1) NQF 7 in Computer Science, Cyber Security or Information and Communication Technology related qualification 2) Certification in Certified Information Systems Security Professional (CISSP) or Certified Information Security Manager (CISM) or Certified Cloud Security Professional (CCSP) or Certified Ethical Hacker or CompTIA Security+ or SABSA or TOGAF or Microsoft Certified or Cybersecurity Architect Expert or GIAC certifications i.e. GDSA 3) An abridged CV indicating at least 5 years' experience in designing, implementing, integrating, and configuring cybersecurity solutions in enterprise environments as described above. 		20.00
CV submitted demonstrating 5 or more years' experience in designing, implementing, integrating, and configuring cybersecurity solutions in enterprise environments cyber security related projects and have the required qualification and certification.	20.00	
CV submitted demonstrating a minimum of 3 years but less than 5 years' experience in designing, implementing, integrating, and configuring cybersecurity solutions in enterprise environments cyber security related projects and have the required qualification and certification.	10.00	
CV submitted demonstrating less than 3 years' experience in in designing, implementing, integrating, and configuring cybersecurity solutions in enterprise environments cyber security related projects and have the required qualification and certification.	0.00	
No CVS, qualification and certification submitted	0.00	

1. DETAILED FUNCTIONALITY EVALUATION CRITERIA:		WEIGHTING ALLOCATED
2. Experience of the Bidder in Similar Work		
Bidders must provide written reference letters (dated not older than five (5) years) on the bidder’s client letterhead, to whom cyber security services are/were provided. The reference letters must include: 1) Contact people and contact details. 2) Confirmation of services rendered; and whether the client/s were satisfied with the service rendered 3) The reference letter must be signed and dated.		30.00
• Three (3) reference letters	30.00	
• Two (2) reference letters	20.00	
• One (1) reference letter	10.00	
• No reference letter	0.00	
3. Methodology and approach		
The approach should focus on pragmatic implementation of controls to achieve the target maturity levels, demonstrating a defense-in-depth set of best practices. The approach must not be generic or artificially intelligent created, it must be specific to FBS demonstrating understanding and knowledge of cyber security.		20.00
Excellent: The proposal is unambiguous and demonstrates a thorough understanding of the requirements and provides full details of how each requirement will be met	20.00	
Good: The proposal meets most of the requirements and is sufficiently detailed to demonstrate a good understanding and provide details of how requirements will be met.	15.00	
Acceptable: The proposal meets some of the requirements and shows an acceptable level of understanding of requirements and provides some satisfactory level of details on how the requirements will be met.	10.00	
Unacceptable: The proposal does not meet any of the above requirements or comply with and/or insufficient/no information provided.	0.00	
TOTAL POINTS		100.00

12.4 Bidder must meet the minimum functionality of **75,00** points out of 100 points in order to be evaluated further. Any bid that does not meet the minimum threshold will not move to the next stage of evaluation.

12.5 Stage 3: Preference Points system

The 80/20 preference points system will be utilized for this bid. This preference points system is for the acquisition of goods or services with a Rand value up to R50 million as follows:

Criteria	Means of verification	Points
Price	Proposed Bid Price	80.00
Preference points	Specific Goals	20.00
Total Points		100.00

12.6 Specific Goals

The following allocation will determine the specific goals for this tender process

Criteria	% Allocation for each category	Points
Black People Ownership (> 50% blacks)	60%	12.00
Women Ownership	30%	6.00
Black Youth Ownership	10%	2.00
Total Points	100%	20.00

12.7 Bidders must submit the following documents as a means of verification for specific goals:

- a) CIPC documents (company registration documents),
- b) A copy of a BBBEE verification certificate or signed affidavit indicating ownership levels,
- c) Shareholder certificates,
- d) Copy(ies) of Identity document(s) for shareholders(s).
- e) Central Supplier Database (CSD) full report. *(Not a summary)*

SECTION C

13. TENDER SUBMISSION INSTRUCTIONS

- 13.1 Tenders should be submitted in triplicate consisting of two hard copies and one electronic copy, all bound in a sealed envelope endorsed, **BID NO: FB SETA (25-26) T0001. THE APPOINTMENT OF A CYBER SECURITY SERVICE PROVIDER FOR A PERIOD OF THREE (3) YEARS.** The sealed envelope must be placed and be deposited in the FoodBev SETA Tender Box, Ground Floor, 7 Wessel St, Rivonia, Sandton, 2128 no later than closing time and date.
- 13.2 Bids must be submitted in a prescribed response format herewith enclosed as 'Response Format'.
- 13.3 The closing date, company name and the return address must also be endorsed on the envelope.
- 13.4 If a courier service company is being used for delivery of the tender document, the tender description must be endorsed on the delivery note/courier packaging and the courier must ensure that documents are placed / deposited into the tender box. FoodBev SETA will not be held responsible for any delays where tender documents are handed to the FoodBev SETA Receptionist and/or arrives late.
- 13.5 No bids received by telegram, telex, email, facsimile, or similar medium will be considered.
- 13.6 Where a tender document is not in the tender box at the time of the tender closing, such a tender document will be regarded as a late tender. FoodBev SETA reserves the right not to consider/evaluate any late tender response.
- 13.7 All the documentation submitted in response to this bid must be in English.
- 13.8 The bidder is responsible for all the costs that they shall incur related to the preparation and submission of the tender document.

- 13.9 Bids submitted by bidders must be signed by a person or persons duly authorised thereto by a resolution of a Board of Directors (if applicable), a copy of which Resolution, duly certified, be submitted with the Tender
- 13.10 Bidders should check the numbers of the pages to satisfy themselves that none are missing or duplicated. No liability will be accepted by FoodBev SETA regarding anything arising from the fact that pages are missing or duplicated.
- 13.11 A valid tax clearance certificate or confirmation of pin must be included in the bid response.
- 13.12 A copy(s) of certificates from the organizations/ bodies that the bidder is affiliated with must be included in the bid response.
- 13.13 FoodBev SETA reserves the right to call bidders for further presentations before awarding.
- 13.14 The onus is on the bidder to provide FB SETA with SAQA evaluation for foreign qualifications. Foreign qualifications not accompanied by SAQA evaluation will not be considered.

14. RESPONSE FORMAT

- 14.1 Bidders are requested to note that this is a guide to responding to the evaluation criteria as detailed above. The soft and hard-copy responses from all bidders must be prepared in line with the following section (each schedule must be clearly marked, indexed and /or numbered):
- 14.2 Cover Page: The cover page must clearly indicate the bid reference number, bid description and the bidder's name.

14.3 Schedule 1:

- a) Executive Summary/Cover Letter – The cover letter should be brief (not more than two pages maximum). Describe why your company/consortium considers it to be best qualified to achieve any of the services listed in scope of work
- b) Brief company profile
- c) Qualifications and Experience – This section shall contain relevant information on qualifications and experience related to the relevant profession. This includes CVs, qualifications and valid certifications.
- d) List of Project team – This list should include the identification of the contact person who will have primary responsibility for the FoodBev SETA contracts, other personnel to be used for project planning, documentation, and supervision, including partners and/or sub-consultants. This must include the organogram.
- e) Reference letters in previous client's letterhead, signed and dated by authorized personnel.
- f) Methodology and approach include an implementation plan that demonstrates the bidder's capacity to deliver the project within the stipulated time frame and budget
- g) Signature Requirements: All bids must be signed. A bid may be signed by an officer or other agent of a registered vendor, if authorised to sign contracts on its behalf; a member of a consortium or joint venture or other agent authorised by a Power of Attorney. The name and title of the individual(s) signing the bid must be clearly shown immediately below the signature.
- h) Rejection of bids: FoodBev SETA reserves the right not to proceed with the award of the proposal.

14.4 Schedule 2:

- a) Valid tax clearance certificate

- b) Certified copies of the bidders CIPC / or company registration documents listing all members with percentages, in case of a CC. Or the latest certified copies of all share certificates in the case of a company.
- c) Originally certified copy of the company's professional accreditation (not a certified copy) if applicable.
- d) Certified ID copies of all directors.
- e) A certified copy of the B-BBEE certificate (or an original affidavit signed by a Commissioner of Oaths regarding the B-BBEE status)
- f) Submission of proof of the bidder's registration on the CSD (Full report)
- g) All tender submissions must include standard bidding documents (SBD documents) duly completed and signed.

Note: If a Consortium, Joint Venture or Subcontractor, the documents listed above must be submitted for each Consortium/ JV member or subcontractor. A consolidated B-BBEE certificate is required for Joint Venture bidders.

15. AUTHORISATION

The BAC committee hereby confirms that the information included in this bid document is agreed upon by all members, compliant, accurate and complete.

SIGNATORIES:

Recommended by the BAC Chairperson: Mr Sinaye Mgidi

Signature: _____ Date: _____

Approved by the CEO: Ms Nokuthula Selamolela

Signature: _____ Date: _____

16. ANNEXURES

ANNEXURE A - GENERAL CONDITIONS OF CONTRACT (GCC)

ANNEXURE B –COMPLIANCE DOCUMENTS AND CONDITIONS TO TENDER

ANNEXURE C- SBD FORMS