



Request for Quotations

Purpose of this Document	The Gauteng Film Commission (GFC) invites suitably qualified and independent cybersecurity service providers to submit quotations for an ICT Security Baseline Assessment and an Independent Website Security Assurance Review. The objective is to identify key security weaknesses across GFC's ICT environment, independently assess selected security controls protecting the public-facing website, and provide a practical, prioritised remediation roadmap. The following documents need to accompany the quotations. - Tax clearance certificate accompanied by a pin for further verification. - Certified BBBEE certificate and CSD Registration number - Completed SBD 4 and SBD 6.1 Completed quotes must be submitted via email to quotes@gautengfilm.org.za by no later than 02 October 2026 at 23:59. Any information contained in the quotes or proposal that is proprietary must be clearly marked as such and will be treated as confidential Technical inquiries should be directed in writing to Mr. Bubele Ngxola bubelen@gautengfilm.org.za
Evaluation Process	PRICE AND BBBEE POINTS The 80/20 preferential point system as per the Treasury Framework Act of 2000 will be applied.

1. Background

The Gauteng Film Commission requires an independent assessment of selected cybersecurity controls within its ICT environment, including independent security assurance over its public-facing web environment. The assessment is intended to provide management with an objective view of the effectiveness of selected security controls, identify material security weaknesses, verify selected corrective actions and establish a prioritised ICT security baseline.

To protect GFC's security information, this public RFQ provides the scope, quantities, activities and deliverables required for pricing but does not disclose detailed technology names, versions, IP addresses, hostnames, architecture, credentials, security findings or detailed corrective-action information. The appointed provider will receive restricted technical information and verification evidence reasonably required to perform the work, subject to confidentiality requirements.

2. Scope of Work

Area	Maximum / pricing basis
Website assurance	One primary public-facing website and its directly supporting hosting/application environment.
Related web component	One related web component/instance, limited to checking material shared-security dependencies where applicable.
Website evidence review	Up to 2 security assessment/corrective-action documents plus the associated action/evidence register supplied by GFC.
ICT baseline assets	Up to 30 priority GFC-managed ICT assets selected by GFC for authenticated vulnerability assessment.
Server baseline	Up to 3 servers, included within the 30-asset limit.
Identity / cloud	One organisational identity/cloud productivity environment; focused configuration review only.
Perimeter security	One primary firewall/perimeter security configuration; read-only review.
Close-out	One management presentation, maximum 2 hours.
Verification follow-up	One evidence-based follow-up verification of up to 5 Critical/High findings, if evidence is supplied within 30 days.

Bidders must price on these assumptions. The scope may not be expanded after appointment without GFC's written approval and an applicable procurement process.

3. Independent Website Security Assurance

The purpose of this service is to independently assess the current security posture of GFC's public-facing web environment and verify selected security controls and corrective actions identified by GFC. The work is a focused assurance assessment and not an open-ended forensic or investigative engagement.

3.1. Review of Security and Corrective-Action Evidence

- 3.1.1. Review up to two security assessment/corrective-action documents and the supporting verification evidence supplied by GFC.

- 3.1.2. Create a concise verification schedule of the material security controls and corrective actions selected by GFC for independent confirmation.
- 3.1.3. Identify material security conclusions or corrective actions that cannot be independently verified from the available evidence.

3.2. Independent Technical Verification

- 3.2.1. Assess the current public-facing website for material known vulnerabilities and insecure configuration using non-destructive automated and manual techniques.
- 3.2.2. Perform targeted website integrity checks, on a risk-based basis, to identify material unauthorised content, unexpected executable/application content, unauthorised configuration or persistence mechanisms within the agreed scope.
- 3.2.3. Review privileged website accounts and effective administrative permissions for unauthorised, excessive or dormant privileged access.
- 3.2.4. Review relevant application/database security controls at a high level, including unnecessary external exposure, privilege and credential-handling controls where evidence/access is provided.
- 3.2.5. Review material persistence areas relevant to the website, including scheduled processes/tasks, remote-management mechanisms and unnecessary/dormant components.
- 3.2.6. Check the primary website and one agreed related component for material shared-security dependencies that could affect the primary website.
- 3.2.7. Review whether key preventative and detective controls are in place, including privileged authentication, patch/update management, perimeter/web protection, logging/alerting and content-integrity monitoring.
- 3.2.8. Review a proportionate sample of available recent website security/log evidence for material indications of unauthorised activity or control failure, where such evidence exists.

3.3. Website Assurance Conclusion

- 3.3.1. The assessor must provide a clear evidence-based conclusion addressing:
 - whether the assessment identified evidence of material unauthorised activity, unauthorised persistence or unauthorised content within the assessed scope;
 - whether the selected security controls and corrective actions reviewed were Verified, Partially Verified, Not Verified or Unable to Verify;

- whether any unresolved Critical/High security weakness materially affects the website security assurance conclusion;
 - whether key preventative and detective controls assessed are operating or require further corrective action; and what residual risks and assessment limitations remain.
- 3.3.2. The provider must not provide a guarantee that the website is free from all security risk or immune from future compromise. The conclusion must be limited to the procedures performed, evidence available and scope assessed.

3.4. Focused ICT Security Baseline

This service is intentionally limited to priority controls and assets. It is not a comprehensive penetration test or full cybersecurity maturity review.

- 3.4.1. Perform authenticated vulnerability scanning of up to 30 priority GFC-managed assets selected by GFC.
- 3.4.2. Validate Critical and High findings to reduce false positives and provide practical remediation actions.
- 3.4.3. Review patch/update posture of up to 3 in-scope servers.
- 3.4.4. Conduct a focused review of privileged administrative access, multi-factor authentication coverage and material identity/security configuration weaknesses in one organisational identity/cloud environment.
- 3.4.5. Conduct a read-only review of one primary perimeter/firewall configuration for material exposure, rule/configuration weaknesses and logging/alerting settings.
- 3.4.6. Review available endpoint-protection coverage/status at a summary level using management evidence; a device-by-device endpoint audit is not required.

3.5. Explicit Exclusions

- 3.5.1. Full internal or external penetration testing involving unrestricted exploitation, lateral movement, or privilege escalation.
- 3.5.2. Digital-forensic reconstruction, historic attack-path investigation or root-cause investigation.
- 3.5.3. Red-team exercises, social engineering, phishing simulations or denial-of-service testing.
- 3.5.4. Wireless penetration testing or source-code review.
- 3.5.5. Full review of every database record, file, log entry or historic backup; verification must be risk-based and targeted.
- 3.5.6. Comprehensive ICT governance/maturity assessment, policy review or compliance certification.
- 3.5.7. Remediation implementation, website development or production configuration changes by the assessor.
- 3.5.8. Managed SOC, recurring monitoring or vulnerability-management services.

3.5.9. Full security assessment of unrelated third-party applications or related websites/components.

3.5.10. Bulk extraction or retention of personal, confidential, or production information.

4. Required Deliverables

Deliverable	Minimum content
1. Website Security Assurance Report	Concise standalone report covering evidence reviewed, verification performed, material current findings, corrective-action status, residual risk, limitations and the independent assurance conclusion required by section 3.
2. ICT Security Baseline Report	Validated priority findings from the 30-asset baseline, server, identity/cloud and perimeter reviews, with risk ratings and remediation recommendations.
3. Consolidated Risk & Action Register	Single register combining material website and ICT baseline findings, priority, recommended action and suggested owner/timeframe.
4. Executive Management Brief	Maximum 5 pages summarising what was independently verified, material outstanding risks, limitations and priority management actions. Suitable for management/governance reporting.
5. Management Presentation	One close-out session of up to 2 hours.
6. Follow-up Verification Note	If applicable, one short verification note for up to 5 Critical/High findings where GFC provides remediation evidence within 30 days.

5. Assessment Approach

5.1. Use non-destructive methods and agree written Rules of Engagement with GFC before active testing.

5.2. Use appropriate automated tools together with manual expert validation; scanner output alone is not an acceptable deliverable.

5.3. Prioritise material risk rather than exhaustive testing of low-risk items.

5.4. Immediately notify GFC ICT of a validated Critical finding presenting an imminent material risk.

5.5. Clearly document assumptions, inaccessible areas, unavailable evidence, and matters that could not be verified.

6. Confidentiality and Controlled Disclosure

- 6.1. The successful bidder must sign applicable confidentiality/non-disclosure requirements before receiving restricted technical or security information.
- 6.2. Detailed platform information, architecture, security assessment documentation, corrective-action evidence, approved configuration information and controlled access will be supplied only after appointment where necessary.
- 6.3. Information may be used only for this assignment and accessed only by authorized assessment personnel.
- 6.4. Credentials and sensitive evidence must not be reproduced unnecessarily in reports and must be securely returned or destroyed after completion.
- 6.5. GFC's security information, findings or technical information may not be published or used as a case study without prior written approval.

7. Minimum bidder requirements

- Valid Tax Compliance Status and Central Supplier Database (CSD) registration.
- Completed SBD 4, SBD 6.1.
- Valid B-BBEE
- At least three comparable cybersecurity vulnerability/security assessment assignments completed within the last five years, supported by references or completion evidence.
- A named lead assessor with relevant hands-on cybersecurity assessment experience.
- At least one relevant recognized cybersecurity qualification/certification within the proposed assessment team.
- Demonstrated capability in public-facing web security assessment and authenticated vulnerability assessment.
- Signed independence/conflict-of-interest declaration, including disclosure of any relationship that may affect the independence of the assessment.

8. Pricing Schedule

Item	Price excl. VAT	VAT	Price incl. VAT
Website security assurance			
Focused ICT security baseline			

PREFERENCE POINTS CLAIM FORM IN TERMS OF THE PREFERENTIAL PROCUREMENT REGULATIONS 2022

This preference form must form part of all tenders invited. It contains general information and serves as a claim form for preference points for specific goals.

NB: BEFORE COMPLETING THIS FORM, TENDERERS MUST STUDY THE GENERAL CONDITIONS, DEFINITIONS AND DIRECTIVES APPLICABLE IN RESPECT OF THE TENDER AND PREFERENTIAL PROCUREMENT REGULATIONS, 2022

1. GENERAL CONDITIONS

1.1 The following preference point systems are applicable to invitations to tender:

- the 80/20 system for requirements with a Rand value of up to R50 000 000 (all applicable taxes included); and

1.2 **To be completed by the organ of state**

(delete whichever is not applicable for this tender).

- a) The applicable preference point system for this tender is the **80/20** preference point system.
- b) The **80/20 preference point system** will be applicable in this tender. The lowest/highest acceptable tender will be used to determine the accurate system once tenders are received.

1.3 Points for this tender (even in the case of a tender for income-generating contracts) shall be awarded for:

- (a) Price; and
- (b) Specific Goals.

1.4 **To be completed by the organ of state:**

The maximum points for this tender are allocated as follows:

	POINTS
PRICE	80
SPECIFIC GOALS	20
Total points for Price and SPECIFIC GOALS	100

1.5 Failure on the part of a tenderer to submit proof or documentation required in terms of this tender to claim points for specific goals with the tender, will be interpreted to mean that preference points for specific goals are not claimed.

Reports, consolidated risk register and executive brief			
Management presentation and included follow-up verification			
TOTAL PRICE			

9. Evaluation and Submission

- Stage 1: Administrative compliance.
- Stage 2: Price and specific goals/preference points
- Technical proposals must state the proposed methodology, project plan, personnel, comparable assignments, assumptions, and exclusions.

- 1.6 The organ of state reserves the right to require of a tenderer, either before a tender is adjudicated or at any time subsequently, to substantiate any claim in regard to preferences, in any manner required by the organ of state.

2. DEFINITIONS

- (a) **“tender”** means a written offer in the form determined by an organ of state in response to an invitation to provide goods or services through price quotations, competitive tendering process or any other method envisaged in legislation;
- (b) **“price”** means an amount of money tendered for goods or services, and includes all applicable taxes less all unconditional discounts;
- (c) **“rand value”** means the total estimated value of a contract in Rand, calculated at the time of bid invitation, and includes all applicable taxes;
- (d) **“tender for income-generating contracts”** means a written offer in the form determined by an organ of state in response to an invitation for the origination of income-generating contracts through any method envisaged in legislation that will result in a legal agreement between the organ of state and a third party that produces revenue for the organ of state, and includes, but is not limited to, leasing and disposal of assets and concession contracts, excluding direct sales and disposal of assets through public auctions; and
- (e) **“the Act”** means the Preferential Procurement Policy Framework Act, 2000 (Act No. 5 of 2000).

3. FORMULAE FOR PROCUREMENT OF GOODS AND SERVICES

3.1. POINTS AWARDED FOR PRICE

3.1.1 THE 80/20 OR 90/10 PREFERENCE POINT SYSTEMS

A maximum of 80 or 90 points is allocated for price on the following basis:

$$\begin{array}{ccc} \mathbf{80/20} & \mathbf{or} & \mathbf{90/10} \\ \\ = (- \frac{\quad}{\quad}) \text{ or } & & = (- \frac{\quad}{\quad}) \end{array}$$

Where

Ps = Points scored for price of tender under consideration

Pt = Price of tender under consideration

Pmin = Price of lowest acceptable tender

3.2. FORMULAE FOR DISPOSAL OR LEASING OF STATE ASSETS AND INCOME GENERATING PROCUREMENT

3.2.1. POINTS AWARDED FOR PRICE

A maximum of 80 or 90 points is allocated for price on the following basis:

$$= \frac{80/20}{\left(\frac{P_t}{P_{max}} \right)} \quad \text{or} \quad = \left(\frac{90/10}{\left(\frac{P_t}{P_{max}} \right)} \right)$$

Where

- Ps = Points scored for price of tender under consideration
Pt = Price of tender under consideration
Pmax = Price of highest acceptable tender

4. POINTS AWARDED FOR SPECIFIC GOALS

- 4.1. In terms of Regulation 4(2); 5(2); 6(2) and 7(2) of the Preferential Procurement Regulations, preference points must be awarded for specific goals stated in the tender. For the purposes of this tender the tenderer will be allocated points based on the goals stated in table 1 below as may be supported by proof/ documentation stated in the conditions of this tender:
- 4.2. In cases where organs of state intend to use Regulation 3(2) of the Regulations, which states that, if it is unclear whether the 80/20 or 90/10 preference point system applies, an organ of state must, in the tender documents, stipulate in the case of—
- (a) an invitation for tender for income-generating contracts, that either the 80/20 or 90/10 preference point system will apply and that the highest acceptable tender will be used to determine the applicable preference point system; or
 - (b) any other invitation for tender, that either the 80/20 or 90/10 preference point system will apply and that the lowest acceptable tender will be used to determine the applicable preference point system,

then the organ of state must indicate the points allocated for specific goals for both the 90/10 and 80/20 preference point system.

Table 1: Specific goals for the tender and points claimed are indicated per the table below.

(Note to organs of state: Where either the 90/10 or 80/20 preference point system is applicable, corresponding points must also be indicated as such.)

Note to tenderers: The tenderer must indicate how they claim points for each preference point system.)

The specific goals allocated points in terms of this tender	Number of points allocated (90/10 system) (To be completed by the organ of state)	Number of points allocated (80/20 system) (To be completed by the organ of state)	Number of points claimed (90/10 system) (To be completed by the tenderer)	Number of points claimed (80/20 system) (To be completed by the tenderer)
HDIs (Who had no franchise on national elections before the 1983 and 1993 constitution) Ownership	4	4		
Women	2	2		
Youth	2	2		
People with disabilities	1	1		
Implementation of RDP goals (The promotion of enterprises located in a specific province for work to be done or services to be rendered in that province) Township	1	1		
		Level1=10 Level2= 9 Level3=8 Level 4=7 Level5=6 Level6=5 Level7=4 Level8=3 Level9=2 Non-Compliant =0		
BBBEEE POINTS	0			

DECLARATION WITH REGARD TO COMPANY/FIRM

- 4.3. Name of company/firm.....
- 4.4. Company registration number:
- 4.5. TYPE OF COMPANY/ FIRM
- Partnership/Joint Venture / Consortium
One-person business/sole propriety

Close corporation
Public Company
Personal Liability
Company (Pty) Limited
Non-Profit Company

State Owned Company
[TICK APPLICABLE BOX]

- 4.6. I, the undersigned, who is duly authorised to do so on behalf of the company/firm, certify that the points claimed, based on the specific goals as advised in the tender, qualifies the company/ firm for the preference(s) shown and I acknowledge that:
- i) The information furnished is true and correct;
 - ii) The preference points claimed are in accordance with the General Conditions as indicated in paragraph 1 of this form;
 - iii) In the event of a contract being awarded as a result of points claimed as shown in paragraphs 1.4 and 4.2, the contractor may be required to furnish documentary proof to the satisfaction of the organ of state that the claims are correct;
 - iv) If the specific goals have been claimed or obtained on a fraudulent basis or any of the conditions of contract have not been fulfilled, the organ of state may, in addition to any other remedy it may have –
 - (a) disqualify the person from the tendering process;
 - (b) recover costs, losses or damages it has incurred or suffered as a result of that person's conduct;
 - (c) cancel the contract and claim any damages which it has suffered as a result of having to make less favourable arrangements due to such cancellation;
 - (d) recommend that the tenderer or contractor, its shareholders and directors, or only the shareholders and directors who acted on a fraudulent basis, be restricted from obtaining business from any organ of state for a period not exceeding 10 years, after the *audi alteram partem* (hear the other side) rule has been applied; and
 - (e) forward the matter for criminal prosecution, if deemed necessary.

.....	
SIGNATURE(S) OF TENDERER(S)	
SURNAME AND NAME:	
DATE:	
ADDRESS:	
	
	
	

BIDDER'S DISCLOSURE

1. PURPOSE OF THE FORM

Any person (natural or juristic) may make an offer or offers in terms of this invitation to bid. In line with the principles of transparency, accountability, impartiality, and ethics as enshrined in the Constitution of the Republic of South Africa and further expressed in various pieces of legislation, it is required for the bidder to make this declaration in respect of the details required hereunder.

Where a person/s are listed in the Register for Tender Defaulters and / or the List of Restricted Suppliers, that person will automatically be disqualified from the bid process.

2. Bidder's declaration

- 2.1 Is the bidder, or any of its directors / trustees / shareholders / members / partners or any person having a controlling interest¹ in the enterprise, employed by the state? **YES/NO**

- 2.1.1 If so, furnish particulars of the names, individual identity numbers, and, if applicable, state employee numbers of sole proprietor/ directors / trustees / shareholders / members/ partners or any person having a controlling interest in the enterprise, in table below.

Full Name	Identity Number	Name of State institution

- 2.2 Do you, or any person connected with the bidder, have a relationship

¹ the power, by one person or a group of persons holding the majority of the equity of an enterprise, alternatively, the person/s having the deciding vote or power to influence or to direct the course and decisions of the enterprise.

with any person who is employed by the procuring institution? **YES/NO**

2.2.1 If so, furnish particulars:

.....

2.3 Does the bidder or any of its directors / trustees / shareholders / members / partners or any person having a controlling interest in the enterprise have any interest in any other related enterprise whether or not they are bidding for this contract? **YES/NO**

2.3.1 If so, furnish particulars:

.....

3 DECLARATION

I, _____ the _____ undersigned,
 (name)..... in
 submitting the accompanying bid, do hereby make the following
 statements that I certify to be true and complete in every respect:

- 3.1 I have read and I understand the contents of this disclosure;
- 3.2 I understand that the accompanying bid will be disqualified if this disclosure is found not to be true and complete in every respect;
- 3.3 The bidder has arrived at the accompanying bid independently from, and without consultation, communication, agreement or arrangement with any competitor. However, communication between partners in a joint venture or consortium² will not be construed as collusive bidding.
- 3.4 In addition, there have been no consultations, communications, agreements or arrangements with any competitor regarding the quality, quantity, specifications, prices, including methods, factors or formulas used to calculate prices, market allocation, the intention or decision to submit or not to submit the bid, bidding with the intention not to win the bid and conditions or delivery particulars of the products or services to which this bid invitation relates.
- 3.4 The terms of the accompanying bid have not been, and will not be, disclosed by the bidder, directly or indirectly, to any competitor, prior to the date and time of the official bid opening or of the awarding of the contract.
- 3.5 There have been no consultations, communications, agreements or arrangements made by the bidder with any official of the procuring

² Joint venture or Consortium means an association of persons for the purpose of combining their expertise, property, capital, efforts, skill and knowledge in an activity for the execution of a contract.

institution in relation to this procurement process prior to and during the bidding process except to provide clarification on the bid submitted where so required by the institution; and the bidder was not involved in the drafting of the specifications or terms of reference for this bid.

- 3.6 I am aware that, in addition and without prejudice to any other remedy provided to combat any restrictive practices related to bids and contracts, bids that are suspicious will be reported to the Competition Commission for investigation and possible imposition of administrative penalties in terms of section 59 of the Competition Act No 89 of 1998 and or may be reported to the National Prosecuting Authority (NPA) for criminal investigation and or may be restricted from conducting business with the public sector for a period not exceeding ten (10) years in terms of the Prevention and Combating of Corrupt Activities Act No 12 of 2004 or any other applicable legislation.

I CERTIFY THAT THE INFORMATION FURNISHED IN PARAGRAPHS 1, 2 and 3 ABOVE IS CORRECT.

I ACCEPT THAT THE STATE MAY REJECT THE BID OR ACT AGAINST ME IN TERMS OF PARAGRAPH 6 OF PFMA SCM INSTRUCTION 03 OF 2021/22 ON PREVENTING AND COMBATING ABUSE IN THE SUPPLY CHAIN MANAGEMENT SYSTEM SHOULD THIS DECLARATION PROVE TO BE FALSE.

.....	
Signature	Date
.....	
Position	Name of bidder