Consultancy Services for Secure Code Review, Penetration Testing, and Patch Support for the In-House Redevelopment of the GSS Website

Terms of Reference

You can access a printable version of the ToR here

1. Project Context

The Ghana Statistical Service (GSS) is currently revamping its official website and data dissemination platform using an internal development team. As the primary repository for national data, the platform's integrity, availability, and confidentiality are paramount.

To minimize risks while supporting innovation, GSS requires a dedicated Security Consultant to implement a DevSecOps approach. This transition involves replacing traditional "end-of-cycle" testing with continuous security assurance integrated into Agile sprint cycles.

During the assignment, the consultant is expected to provide training and knowledge transfer to the GSS development team on the project.

2. Purpose of the Activity

The primary goal is to provide **independent security assurance** while fostering a culture of secure coding within the GSS development team.

Strategic Objectives:

- **Shift-Left Security:** Identify vulnerabilities during the coding phase rather than post-deployment.
- **Validation:** Execute rigorous penetration testing to simulate real-world attacks.
- **Remediation Support:** Provide "hands-on" patch guidance to ensure vulnerabilities are not just identified but closed.
- **Knowledge Transfer:** Improve the GSS development team’s capability in secure SDLC (Software Development Life Cycle) practices.

3. Scope and Content of the Assignment

The consultancy is structured into three integrated work streams, mapped to GSS’s Agile delivery model.

3.1 Agile-Aligned Secure Code Analysis (SAST/DAST)

The consultant shall perform continuous Static Application Security Testing (SAST) and manual code reviews:

- *Sprint Integration:* Review code changes for every major Pull Request (PR) or at the end of each two-week sprint.
- *Vulnerability Focus:* Mitigate OWASP Top 10 risks, including SQL Injection, Cross-Site Scripting (XSS), Broken Access Control, and Insecure Decryption.
- *SCA (Software Composition Analysis):* Audit third-party libraries and dependencies for known vulnerabilities (CVEs).

3.2 Penetration Testing (VAPT)

The consultant shall conduct Black-box and Grey-box testing on staging and production-ready environments:

- *Logic Testing:* Beyond automated scans, the consultant must test business logic flaws (e.g., unauthorised data access between different statistical tiers).
- *API Security:* Specific focus on the REST/GraphQL endpoints used for data dissemination.
- *Reporting:* Deliver a comprehensive report including *Proof of Concept (PoC)* for every "High" or "Critical" finding.

3.3 Patch Support and Remediation Tracking

Unlike traditional audits, this role requires active participation in the fix:

- *Ticket Integration:* Translate findings directly into the team’s backlog.
- *Direct Guidance:* Provide code snippets and configuration templates to remediate identified flaws.
- *Verification:* Perform regression testing to ensure patches do not introduce new vulnerabilities.

4. Key Deliveries and Timelines

The Consultant must start no later than April 2026. The consultancy is expected to commence after each biweekly sprint phase. The final Assurance report (Deliverable D5) should be submitted no later than August 2026.

In each sprint the consultant is expected to spend four to eight (4-8) working hours with the GSS development team. The number of days should be seen as an average as the GSS team is expected to need less support as the project progresses.

The expected deliverables are:

Deliverable	Description	Timeline
D1: Inception Report	Rules of Engagement (RoE), communication protocols, and toolsets.	5 Days post-award
D2: Sprint Security Memos	Bi-weekly summaries of code vulnerabilities and "quick-fix" patches.	Two days after of every Sprint
D3: Full Pentest Report	Deep-dive analysis of the staging environment with PoCs.	Two weeks after a Major Release
D4: Remediation Log	A live tracker showing 'Open', 'In-Progress', and 'Verified' flaws.	Ongoing
D5: Final Assurance Report	Detailed report of the security posture and "Go/No-Go" recommendation.	5 Days before Launch

The consultant is not responsible for:

- Developing new functional features
- Managing cloud hosting, billing or infrastructure procurement
- Content migration or SEO
- Structuring or facilitating “sprints”

5. Confidentiality

All materials produced or acquired under this consultancy shall be treated as strictly confidential and shall not be disclosed to any third party without the prior written consent of Statistics Denmark (SD) and Ghana Statistical Service (GSS)
A strict Non-Disclosure Agreement (NDA) shall be signed. No GSS data may be stored on the consultant's personal/unencrypted devices.

The NDA applies to the Consultant as a whole and to all staff involved in the project. All staff members of the consultancy firm must sign an NDA before gaining access to GSS systems and code.

Ownership: All scripts, reports, and code patches developed during this contract remain the exclusive property of the Ghana Statistical Service.

6. Budget

The consultant will be engaged on a biweekly basis from April to August 2026 to support secure code review, penetration testing, and remediation guidance aligned with the Agile sprint cycles. Given the time frame the Consultant should plan and budget for no more than 10 sprint cycles.

7. Reporting and Institutional Arrangement

One of the objectives of the assignment is to transfer knowledge to the GSS development team. The Consultant is therefore to engage with the GSS development team.

Direct Report: The Consultant shall report to:

Director
Information Technology Services
Ghana Statistical Service
Mark Abuabu-Dadzie
mbuabu-dadzie@statsghana.gov.gh

All written communications to the Director of Information Technology Services should have the GSS technical lead in CC:

Kwesi Eshun
kwesi.eshun@statsghana.gov.gh,

Emergency Protocol: "Critical" vulnerabilities (Exploitable in the wild) must be reported via an encrypted channel (email) within ***4 hours*** of discovery.

The actual contract will be between Statistics Denmark on behalf of GSS and the Consultant.

8. Duration of Consultancy

The consultancy is expected to commence in April 2026 and conclude in August 2026 with the delivery of D5. The deadline for submission of proposal and quotations for this assignment is April 10 - 2026

9. Technical Requirements & Educational Qualifications

The Lead Consultant/Firm must demonstrate:

Web Application Security Testing

- Proven ability to perform comprehensive security assessments and penetration testing for web applications.
- Experience identifying and mitigating vulnerabilities such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), authentication flaws, and other common web security risks.

Secure Development and Code Review

- Ability to conduct detailed code analysis and review to identify security weaknesses and recommend improvements.
- Experience working within Agile development environments and supporting developers with secure coding practices.

Technology Stack Expertise

- Strong technical proficiency in modern web development technologies including *React, Node.js, Python/Django, and PostgreSQL.*
- Ability to review system architecture and application components built using these technologies.

Knowledge Transfer and Capacity Building

- Demonstrated experience in providing structured technical feedback and guidance to the development team.
- Ability to support GSS development team through technical briefings, documentation, and practical recommendations.
- Certifications: Minimum of OSCP (Offensive Security Certified Professional) or CISSP for leads; GWAPT or CEH Master for testers.
- Experience: At least 5 years in securing high-traffic government or financial web platforms.

Educational Qualification

- A minimum of a Bachelor's degree in Computer Science, Information Technology, Cybersecurity, Software Engineering, or a related field from a recognized institution.
- A Master's degree in Cybersecurity, Information Security, Computer Science, or a related discipline will be considered an advantage.

10. How to Apply

The proposal should contain the following:

- How qualifications are met
- Demonstrate experience with similar or comparable assignments
- Description of the planned process for undertaking the assignment, outlining a detailed project work plan
- Description of deliverables
- Budget – including a breakdown of expected work days for each deliverable

Send your application to:

Statistics Denmark:
Chief Adviser Jesper Ellemose Jensen, Statistics Denmark.
jej@dst.dk
Subject line: Secure Code Review, Penetration Testing,
The email should have:
Senior Adviser and Project Manager Emil Aurehøj Persson eap@dst.dk in CC

11. Contact information

Statistics Denmark:
Chief Advisor
Jesper Ellemose Jensen, Statistics Denmark.
jej@dst.dk
WhatsApp: +45 4051 3056

Ghana Statistical Service:
Project Lead
Kwesi Badu Eshun
email: kwesi.eshun@statsghana.gov.gh
mobile: 0244893718

12. Technical Evaluation and Selection Criteria

This matrix below will be used to ensure the winning bidder has both theoretical knowledge and practical agile experience to collaborate effectively with the development team.

Criteria	Weight	Evaluation Sub-Criteria
1. Institutional Experience	20%	• Evidence of at least 5 years in cybersecurity consulting. • Proven track record with government or public sector data platforms. • Experience with Statistical or Data-heavy web applications.
2. Technical Proficiency	30%	• Demonstrated expertise in SAST/DAST tools (e.g., SonarQube, Snyk, Burp Suite Professional). • Experience with GSS's specific tech stack (e.g., React, Node.js, Python). • Ability to provide manual code review beyond automated scans
3. Methodology & Approach	20%	• Alignment with Agile/Scrum (how they fit into 2-week sprints). • Clarity of the "Rules of Engagement" for penetration testing. • Quality of sample remediation reports/logs.

4. Personnel Qualifications	15%	• Lead Consultant: OSCP, CISSP, or CISM certifications. • Technical Team: Evidence of GWAPT (Web App Penetration Tester) or equivalent. • Experience in DevSecOps integration.
5. Knowledge Transfer	15%	• Proposed plan for upskilling GSS in-house developers. • Availability for "Office Hours" or technical workshops during the contract.

Scoring Guide

0-50%: Does not meet requirements; lacks specific experience in Agile security.

51-75%: Meets basic requirements but lacks deep "Shift-Left" integration experience.

76-100%: Demonstrates exceptional technical depth, relevant certifications, and a clear roadmap for supporting the in-house team.