Procurement Statement of Work

FILLED EXAMPLE

Penetration Testing Services — Customer Portal Modernization

Project: CPM-2026 · Version: 1.0 · Owner: M. Tanaka (PM) / S. Eriksen (Procurement) · Date: 2026-09-18

1. CONTRACTING PARTIES & SOW REFERENCE

SOW reference	SOW-CPM-2026-07 (issued under MSA-2024-SEC-044)
Effective date	2026-09-18
Engagement term	2026-10-01 through 2026-11-15 (testing window); warranty through 2027-02-28
Buyer	Meridian Commercial Bank, N.A. — 1 Harbour Plaza, 15F, Singapore 049315
Seller	Ironwall Security Ltd. — 220 Clerkenwell Road, London EC1R 5QT, United Kingdom
Programme linkage	Charter CPM-2026 (Customer Portal Modernization); pre-launch security gate G-04
Buyer authorisation	R. Patel, VP Digital Channels (Sponsor); M. Tanaka, PMP (Project Manager)

2. BACKGROUND & PURPOSE

The Customer Portal Modernization programme (CPM-2026) is scheduled to enter production on 2026-12-06 and must satisfy the 2026 regulator mandate for strong customer authentication and open-banking API surface. Buyer's Security Office requires an independent, adversarial assessment of the new portal, its six open-banking APIs, and the Identity & Access Management (IAM) integration prior to Go/No-Go (milestone 2026-11-08). Seller is a CREST- and CBEST-accredited specialist in financial-services penetration testing and has been selected from the Buyer's approved panel following a competitive three-bid evaluation recorded in Procurement file PR-2026-3117. This Statement of Work authorises Seller to perform a grey-box web application and API penetration test, an authenticated IAM flow test, and a remediation retest, culminating in a findings package sufficient for the Buyer Security Office to sign off security gate G-04.

3. SCOPE OF WORK

3.1 In scope

- Grey-box web application penetration test of the customer-facing portal (staging URL: portal-stg.meridian.example), including all authenticated user flows (login, statements, transfers, cards, alerts, beneficiaries).
- API penetration test of the six open-banking APIs (accounts, balances, transactions, payments-initiation, beneficiaries, standing-orders) against OWASP API Security Top 10 (2023).
- Authenticated flow testing of the IAM integration (TOTP and SMS-fallback MFA), session management, token lifetimes, and account recovery.
- Business-logic testing of payment-initiation flows, including idempotency, replay, and race-condition scenarios.
- Infrastructure reconnaissance limited to Buyer-issued target list; TLS configuration review; WAF bypass attempts against the staging ingress.
- One (1) remediation retest of High/Critical findings, scheduled within 21 calendar days after delivery of the Final Report.

3.2 Out of scope

- Denial-of-service, volumetric, or stress testing of any Buyer environment.
- Social engineering, phishing of Buyer staff, or physical security assessments.
- Source-code review (white-box) — commissioned separately under SOW-CPM-2026-05.
- Testing of the production environment, core banking systems, or third-party SaaS providers not explicitly listed in the target schedule.

Procurement Statement of Work

FILLED EXAMPLE

Penetration Testing Services — Customer Portal Modernization

Project: CPM-2026 · Version: 1.0 · Owner: M. Tanaka (PM) / S. Eriksen (Procurement) · Date: 2026-09-18

- Native mobile applications (covered under programme MOB-2026).

3.3 Assumptions

- Buyer will provide four (4) pre-provisioned test identities with differing entitlements by 2026-09-28.
- The staging environment will be functionally equivalent to production, data-masked, and stable throughout the testing window.
- Buyer's SRE team will make best-effort for 4-hour recovery of staging if Seller's testing induces an outage.
- All findings are owned by the Buyer; Seller retains no copies after the destruction obligation in section 12.

4. DELIVERABLES

ID	Deliverable	Acceptance criteria	Due date	Format
D-01	Engagement kick-off pack & rules of engagement	Scope, targets, contacts, escalation paths, and testing windows signed by both parties; Buyer IR team briefed.	2026-10-03	PDF + signed memo
D-02	Detailed test plan & methodology	Mapped to OWASP ASVS L2 and OWASP API Top 10; Buyer Security Office review with no open objections.	2026-10-08	PDF (encrypted)
D-03	Interim findings report (week 2)	All Critical/High findings disclosed within 24 hours of discovery; interim report delivered end of testing week 2.	2026-10-23	PDF (encrypted)
D-04	Final penetration-test report	Executive summary + technical detail; every finding has CVSS v3.1 score, reproduction steps, evidence, and remediation guidance; zero P0 quality defects from Buyer review.	2026-11-06	PDF (encrypted) + JSON export
D-05	Executive summary briefing	Live 60-minute briefing to Buyer's sponsor, CISO, and Go/No-Go board; slide deck delivered in advance.	2026-11-09	Slide deck + live session
D-06	Remediation advisory log	Written advisory on Buyer-proposed fixes for each High/Critical finding, within 3 business days of Buyer request.	Rolling through 2026-11-13	Email + tracker entries
D-07	Retest report	All High/Critical findings retested; each marked Fixed / Partially Fixed / Not Fixed with evidence; Buyer sign-off on security gate G-04.	2026-11-15	PDF (encrypted)
D-08	Data-destruction certificate	NIST SP 800-88 compliant wipe of all Buyer data from Seller systems; signed certificate delivered.	2026-11-30	Signed PDF

5. SCHEDULE & MILESTONES

Milestone	Target date	Owner	Dependency
SOW executed by both parties	2026-09-25	S. Eriksen	—

Procurement Statement of Work

FILLED EXAMPLE

Penetration Testing Services — Customer Portal Modernization

Project: CPM-2026 · Version: 1.0 · Owner: M. Tanaka (PM) / S. Eriksen (Procurement) · Date: 2026-09-18

Milestone	Target date	Owner	Dependency
Kick-off meeting & rules of engagement signed	2026-10-01	H. Okonkwo (Seller)	SOW signature
Testing window opens	2026-10-05	H. Okonkwo	Test accounts provisioned
Interim findings report	2026-10-23	H. Okonkwo	Week-2 testing complete
Testing window closes	2026-11-02	H. Okonkwo	—
Final report delivered	2026-11-06	H. Okonkwo	Testing complete
Executive briefing to Go/No-Go board	2026-11-09	H. Okonkwo / M. Tanaka	Final report
Retest & gate G-04 sign-off	2026-11-15	Security Office	Fixes deployed to staging
Data destruction certified	2026-11-30	Seller CISO	Retest complete

6. SERVICE LEVELS & PERFORMANCE STANDARDS

- Critical (CVSS "e 9.0) findings disclosed to Buyer within 4 hours of confirmed exploitation; High findings within 24 hours.
- Seller response to Buyer enquiries during the testing window: acknowledgement within 2 business hours, substantive response within 1 business day.
- Final report quality: zero Buyer-assessed P0 quality defects (missing reproduction steps, missing CVSS, unredacted PII) on first submission; up to one revision cycle permitted within 3 business days.
- All test traffic tagged with the agreed X-Pentest header and source IPs; any untagged destructive action is a material breach.
- Named key personnel (section 11) present at kick-off, interim review, and executive briefing; "e 80% of billed testing effort performed by named staff.
- Confidentiality: all Buyer material handled at Seller's ISO 27001-certified facilities; no offshore processing without written Buyer consent.

7. PRICING & PAYMENT TERMS

7.1 Price type and total

Price type	Firm Fixed Price (FFP). No T&M element. Out-of-scope work only by signed amendment under section 10.
Total contract value	USD 78,500 (seventy-eight thousand five hundred United States dollars), exclusive of VAT/GST.
Currency & FX	USD; payable by SWIFT to Seller's nominated account. No FX adjustment.
Taxes	Each party bears its own income taxes. Buyer will apply Singapore GST reverse-charge per local rules; Seller's invoice must quote its UK VAT number (GB 413 552 908).

Procurement Statement of Work

FILLED EXAMPLE

Penetration Testing Services — Customer Portal Modernization

Project: CPM-2026 · Version: 1.0 · Owner: M. Tanaka (PM) / S. Eriksen (Procurement) · Date: 2026-09-18

Expenses	Not separately reimbursable. All travel, tooling, and incidentals included in the FFP.
Invoicing	Invoices addressed to Accounts Payable, Meridian Commercial Bank, via ap-portal.meridian.example (PO #PR-2026-3117). Net 30 days from invoice acceptance.

7.2 Payment schedule

#	Trigger / deliverable	% of total	Amount (USD)	Net terms
1	Kick-off complete; D-01 accepted (2026-10-03)	20%	15,700.00	Net 30
2	Final penetration-test report D-04 accepted by Buyer Security Office	60%	47,100.00	Net 30
3	Retest report D-07 accepted and gate G-04 signed off	20%	15,700.00	Net 30
	Total	100%	78,500.00	

The total contract value of USD 78,500 falls within the Project Manager's delegated vendor authority ("d USD 50,000 per SOW) only when read with the sponsor's written co-approval dated 2026-09-15 (file PR-2026-3117). Co-approval is recorded as a condition precedent to execution.

8. ROLES & RESPONSIBILITIES

Role	Buyer responsibility	Seller responsibility	Contact
Engagement sponsor	Approve scope, funding, and escalations.	—	R. Patel (Buyer)
Project manager	Day-to-day coordination, acceptance, schedule.	—	M. Tanaka (Buyer)
Security lead	Approve test plan; own findings triage.	Lead consultant for technical dialogue.	D. Ayalew (Buyer) / H. Okonkwo (Seller)
SRE / platform	Provision staging; on-call during test window.	Comply with rules of engagement; no prod testing.	T. Okafor (Buyer)
Procurement & legal	Issue PO; execute SOW and amendments.	Counter-sign; provide insurance certificates.	S. Eriksen (Buyer)
Incident response	Stand-by IR bridge during test window.	Immediate notification of any accidental impact.	CSIRT (Buyer) / Seller duty officer

9. ACCEPTANCE PROCEDURE

Each deliverable is reviewed by the Buyer Security Office within five (5) business days of receipt. Acceptance is evidenced by a signed acceptance memo (template MSA-Ex-B). If a deliverable is rejected, Buyer shall provide a written defect list; Seller shall re-submit within three (3) business days. A second rejection escalates to the joint governance meeting (Buyer PM + Seller engagement director) within three (3) business days; unresolved disputes follow section 15. Deemed acceptance does not apply — silence is not acceptance.

Procurement Statement of Work

FILLED EXAMPLE

Penetration Testing Services — Customer Portal Modernization

Project: CPM-2026 · Version: 1.0 · Owner: M. Tanaka (PM) / S. Eriksen (Procurement) · Date: 2026-09-18

10. CHANGE CONTROL

Any change to scope, deliverables, schedule, key personnel, or price is proposed in writing by either party as a Change Request. Seller provides an impact estimate (effort, price, schedule) within three (3) business days. Changes take effect only upon a signed written amendment to this SOW executed by the same authorised signatories. Work performed on an unsigned change is at Seller's risk and is not billable.

11. KEY PERSONNEL

The following Seller personnel are designated Key Personnel. Substitution requires Buyer's prior written approval (not unreasonably withheld); a substitute must have equivalent or greater certifications and demonstrable financial-services experience.

Name	Role	Seniority / certifications	Allocation
H. Okonkwo	Engagement Lead / Principal Consultant	OSCE3, CREST CCT-APP, 12 yrs fin-svcs	60% through window
P. Volkov	Senior Web & API Tester	OSWE, CREST CRT, 8 yrs	100% through window
C. Marín	Senior IAM & Business-Logic Tester	OSCP, CREST CRT, 7 yrs	80% through window
N. Haddad	Report Lead & QA	OSCP, CISSP, 10 yrs	40% through window

12. CONFIDENTIALITY, IP, DATA HANDLING & SECURITY

- Confidentiality per MSA-2024-SEC-044 § 8; survives termination for five (5) years. All deliverables marked 'Meridian Confidential — Security'.
- Intellectual property: all Buyer data and deliverable content are Buyer's property. Seller retains rights to its pre-existing methodologies and generic tooling; a non-exclusive licence is granted to Buyer for internal use of any embedded Seller material.
- Data handling: no Buyer data is removed from Seller's ISO 27001 UK facilities. Findings are stored encrypted at rest (AES-256) and transmitted via Buyer's SFTP / PGP-encrypted email only.
- No production Buyer data (PII, account numbers, balances) shall be retained beyond the testing window. Seller shall sanitise all engagement data per NIST SP 800-88 by 2026-11-30 and deliver D-08.
- Personnel: all Seller staff assigned to this engagement have passed BS 7858 / equivalent background checks and signed individual NDAs aligned to the MSA.
- Any suspected or confirmed incident involving Buyer data is reported to the Buyer CSIRT within 24 hours; Seller co-operates fully with Buyer and regulator notifications.

13. WARRANTIES & LIABILITY

Seller warrants that services will be performed by suitably qualified personnel in accordance with good industry practice, that deliverables will materially conform to section 4, and that Seller's work will not knowingly introduce malicious code into Buyer systems. Buyer's sole remedy for breach of this warranty is re-performance of the defective service at no additional charge, provided written notice is given within sixty (60) days of delivery. Liability is capped per MSA-2024-SEC-044 § 11 at two times the total contract value (USD 157,000); standard carve-outs apply for confidentiality breach, wilful misconduct, fraud, and indemnity for third-party IP infringement.

Procurement Statement of Work

FILLED EXAMPLE

Penetration Testing Services — Customer Portal Modernization

Project: CPM-2026 · Version: 1.0 · Owner: M. Tanaka (PM) / S. Eriksen (Procurement) · Date: 2026-09-18

14. TERMINATION

- For convenience: Buyer may terminate on fifteen (15) days' written notice; Buyer pays for deliverables accepted and work-in-progress on a pro-rata basis, capped at the next unpaid milestone.
- For cause: either party may terminate on written notice if the other commits a material breach not cured within ten (10) business days of written notice, or becomes insolvent.
- On termination Seller ceases all testing, returns Buyer materials, and completes the data-destruction obligations in section 12 within ten (10) business days.

15. GOVERNING LAW, DISPUTE RESOLUTION & JURISDICTION

Governing law	Laws of Singapore, excluding conflict-of-laws rules.
Dispute resolution	Good-faith executive escalation (15 business days); then binding arbitration under SIAC Rules, seat Singapore, single arbitrator, English language.
Jurisdiction	Singapore International Commercial Court for any matter not subject to arbitration (e.g., injunctive relief for confidentiality).
Notices	Buyer: legal@meridian.example; Seller: contracts@ironwall.example — with copy by registered post to the addresses in section 1.

APPROVALS

For Buyer — Sponsor

R. Patel
VP, Digital Channels, Meridian Commercial Bank

Signature

Date

For Seller — Authorised Signatory

G. Alvarez
Chief Commercial Officer, Ironwall Security Ltd.

Signature

Date

Buyer — Procurement

S. Eriksen
Head of IT Procurement

Signature

Date

Seller — Engagement Director

H. Okonkwo
Principal Consultant & Engagement Lead

Signature

Date