PASC
PAN-AFRICAN STANDARDS COUNCIL

CURRICULUM / INSTITUTIONAL EDITION

PASC-OSPCRM-PENTEST-01 · ED. 1.0 · NOVEMBER 2026

Advanced penetration testing and predictive risk qualification

Prerequisites · Complex scenarios · Predictive model qualification

Issuing authority
Pan-African Standards Council (PASC)

Publication status
Published training curriculum

Publication date
1 November 2026

1. Programme objective

This curriculum prepares experienced security practitioners to plan and execute authorized adversarial examinations, build demonstrable predictive risk models and provide evidence-based remediation decisions across complex environments. Qualification is earned through independent practical examination at a PASC-accredited examination partner.

2. Admission thresholds

Applicants SHALL complete every admission gate in PASC OSPCRM QUAL 01 section 4: verified CompTIA Security+ or an equivalent security-foundations assessment, recognized ethical-hacking competence supported by actual exploitation and reporting work, authorization and confidentiality obligations, and eligibility testing where equivalent credentials are used. Security foundations and ethical-hacking practical equivalence each require at least **85%**. Safety and scope controls require **100%**.

3. Curriculum architecture

Module	Applied learning outcomes	Evidence submitted
01. OSPCRM foundations	Mission consequence, P0–P4, risk owners, assets, contextual dimensions, FNR and P0 precision	Context and priority map; baseline controls matrix
02. Rules of engagement	Legal authority, target scope, evidence stewardship, stop rules, safe rollback	Signed engagement scope, safety rehearsal and cleanup report
03. Identity, networks and exploitation	Enumerate and validate attack paths in AD, OIDC/SAML, VPN, privileged access and segmented networks	Authorized exploit chain with precise log and evidence markers
04. Cloud, container and API security	Cross-plane risks in cloud IAM, Kubernetes, pipelines, GraphQL/REST and service accounts	Multistage cloud/API chain and attack narrative
05. Threat modelling and adversarial adaptation	Attacker objectives, privilege transitions, lateral movement, supplier and insider paths	Threat graph, trust boundaries and alternative attack paths
06. Predictive cyber-risk modelling	Construct model, contextual features, uncertainty, holdout validation and calibration	Executable model, dataset documentation, confusion matrix, FNR and P0 precision
07. Offensive-to-defensive verification	Independently test containment, preventative controls, detection and response	Closure criteria and observed-control validation
08. AI and agentic attack surfaces	Prompt/data manipulation, unsafe authority, training/data exposure, model evaluation	AI attack-case report mapped to PASC AI 01 and OSPCRM

Module	Applied learning outcomes	Evidence submitted
09. Quantum cryptographic transition	Find vulnerable trust paths, build CBOM, prioritize HNDL, simulate cryptographic migration failure	CBOM extract, transition decision and Q01 acceptance tests
10. Sovereignty and dependencies	Jurisdictional dependency, external control planes, key custody, supplier reversibility	Supplier-risk and operational sovereignty assessment
11. Advanced reporting and expert examination	Explain risk to technical and executive audiences with reproducing evidence	Audit-ready report, quantified exposure and executive decision brief
12. Capstone challenge	Apply integrated methodology on changing adversarial scenarios and demonstrate independently valid risk classification	Timed practical exam, completed model, findings and independent review

4. Scenario library and progression

Foundation exercise: examiner-defined asset inventory, multiple weak signals and an authorized test scope. Candidate identifies priorities, evidence gaps and plausible attacker paths.

Complex exercise A: federated identity compromise propagates through cloud identity, API access, container execution and business data. Assess detection and hardening across the chain.

Complex exercise B: supplier software updates introduce a malicious component and a misleading vulnerability severity. Candidate builds an alternative attack graph, quantifies dependencies and reprioritizes P0/P1 exposure.

Complex exercise C: data-protection and critical-service constraints require choosing a safe path under changing attacker behavior. Candidate must preserve evidence and verify remediation.

Complex exercise D: cryptographic migration combines PQC interoperability, rollback weaknesses, signature trust-chain error and potential harvest-now-decrypt-later exposure. Candidate documents control failure and realistic migration acceptance criteria.

Predictive challenge: held-out incidents and adversarial changes require a calibrated model, measured FNR and P0 precision, false-positive tradeoffs, confidence estimates, drift detection and written explanation of the model’s limits.

5. Independent examination

The written component evaluates architecture, threat mechanics, model calibration, evidence quality, OSPCRM risk method and ethical controls. The practical component contains at least four active multistage scenario families, distinct from training labs, and a held-out predictive dataset. Candidate decisions are individually logged, and the rubric assigns points to discovery, accurate reasoning, safe execution, model results, technical evidence and remediation validation.

The minimum is **85% theory**, **85% practical**, **85% predictive component**, **80% in every critical competence section**, **100% of mandatory evidence** and zero critical safety or integrity breaches. A target of **FNR ≤10%** and **P0 precision ≥90%** applies to the independently labelled controlled examination dataset. Equivalent pass conditions cannot be obtained by averaging away a failed critical domain.

6. Examiner controls and accreditation

The examiner SHALL be associated with a PASC-accredited examination partner, independent of the candidate's sole training instructor, and use a controlled assessment bank with separate seeds and cases. Examination accounts, infrastructure and materials SHALL be segregated from public training use. Each run SHALL create reproducible logs, controlled grade sheets, reviewer notes, chain of custody, result identity and a documented appeal route.

Training providers seeking accreditation SHALL satisfy PASC OSPCRM QUAL 01 section 6, including ISO-level eligibility, coverage of all claimed programmes, verified instructor competence, examination independence, actual service-delivery records, quality cycles and complete mandatory-control coverage.

7. Candidate output pack

1. Rules of engagement and authorized target scope.
2. Asset/service inventory and OSPCRM classification.
3. Threat model and exploitable paths with reproducibility evidence.
4. Technical logs, screenshots and data-protection controls as permitted.
5. Predictive model and holdout test results, including FNR, P0 precision and calibration.
6. AI/quantum/dependency cross-mappings where scenarios require them.
7. Prioritized remediation and verified closure evidence.
8. Full technical report, executive brief and examiner evaluation result.

8. Certificate record

A successful candidate receives a **Certified** record describing the OSPCRM qualification scheme, issuing accredited examination partner, assessed competence profile, effective period and verification reference. The record is neither a product conformance statement nor the accreditation of the candidate's employer.

Annex — Glossary

FNR: false-negative rate, missed truly positive cases divided by all truly positive cases in the labelled evaluation population. **P0 precision:** fraction of predicted P0 cases confirmed as genuinely P0 by the examination ground truth. **HNDL:** harvest now, decrypt later. **CBOM:** cryptographic bill of materials. **Holdout set:** cases excluded from model training and threshold selection. **Risk owner:** accountable party accepting and treating actual risk under the organization’s approved governance.