Security Firm Certifications — What Buyers Require

Security Firm Certifications — What Buyers Require

Context: Enterprise and government buyers require specific certifications before signing pen-test or security audit contracts. ISO 9001 + ISO 27001 alone are NOT sufficient — they prove quality management and ISMS baseline but do NOT demonstrate offensive security capability.

Organizational Standards (Firm-Level)

CREST (UK/Global)

De-facto industry standard. Banks, finance sector, and EU enterprise require CREST member status. https://www.crest-approved.org

CHECK (UK NCSC)

Mandatory for UK government contracts.

PCI QSA + PCI ASV

Mandatory for payment-card scope (Visa/Mastercard merchants). Firms must be PCI-certified to issue compliance reports.

CBEST (UK BoE) / TIBER-EU (ECB)

Financial-sector red-team framework. Required for Threat-Led Penetration Testing (TLPT) under DORA regulation (Jan 2025).

SOC 2 Type II

Operational control certification. US enterprise buyers require this.

ISO 27001 + ISO 27701

ISO 27001 = Information Security Management System baseline. ISO 27701 = privacy extension for GDPR/ESG compliance. Required but NOT sufficient on their own.

Norwegian Context

NSM Sikkerhetsgodkjent

Mandatory for classified work (government, defense sector). Access restricted to accredited firms only. Certification journey takes 12-24 months.

DNV or Nemko ISMS Audit

Accredited assessors for Norwegian ISO 27001 certification.

Individual Tester Certifications (Team-Level)

Firms must employ certified individuals to demonstrate technical capability:

- **OSCP (Offensive Security Certified Professional)** — Minimum credibility for junior pen-testers.
- **OSEP / OSWE / OSED** — Advanced certifications (exploitation, web app, exploit development).
- **CREST CRT / CCT** — Mapped to CREST organizational membership requirements.
- **GPEN, GXPN, GWAPT (SANS)** — Enterprise buyers recognize SANS certifications.
- **CISSP** — Management-level security perspective.

Practical Minimum for Serious Buyer (2026)

1. ISO 27001 (firm-level)
2. CREST member status (or national equivalent)
3. OSCP for core team + at least 1 senior with OSEP/OSCE3/CRT
4. PCI ASV if client has payment-card scope
5. NDA + cyber liability insurance (5-10M USD coverage minimum)

⚠ **Reality Check:** Enterprise clients will NOT sign a pen-test contract without CREST (or equivalent) + proof of individual certifications on the team.

Related: Outsource Models, Legal & Marketing Constraints

Source: MC #10446, CEO email 2026-05-01 (Message-ID 2507b6c1)

Revision #3
Created 2026-05-01 19:14:02 UTC by John
Updated 2026-06-07 20:00:53 UTC by John