ALAI Sec Service Line Strategy

Strategic documentation on security service line outsource models, certifications, and go-to-market planning.

- Security Firm Certifications — What Buyers Require
- Norwegian Security Market Landscape
- Outsource Models — Referral / White-label / Managed Service
- Legal & Marketing Constraints When Outsourcing Security
- Practical First Steps + Partner Selection Red Flags

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)

Norwegian Security Market Landscape

Norwegian Security Market Landscape

Context: Factual overview of the Norwegian cybersecurity market. This is NOT a deep market analysis — it provides orientation on existing players, regulatory drivers, and potential gaps. For authoritative market data, refer to NSM yearly threat assessment (nsm.no), Cybersecurity Norway market reports, IKT-Norge security working group.

Major Players

Large Enterprise Providers

- **Mnemonic** — ~500+ employees, dominant enterprise MSSP (Managed Security Service Provider)
- **Watchcom Security** — Telenor Group subsidiary
- **Netsecurity**
- **Defendable**
- **Truesec Norge** — Swedish origin, Norwegian operations

Big Four Advisory

- KPMG / PwC / EY / Deloitte security advisory wings

IT Consulting Firms with Security Wings

- Sopra Steria
- Bouvet
- Atea

Defense Sector

- Combitech (SAAB Norge)

NSM-Godkjent Offensive Security List

Approximately 10-15 firms hold full security clearance for government contracts. Entry barrier: 12-24 month certification journey.

Market Drivers (2026)

- **NIS2 Directive** — Norwegian implementation active 2025. Exponential demand for compliance audits.
- **DORA (Digital Operational Resilience Act)** — Financial sector, Jan 2025. Banks and insurance companies must conduct TLPT (Threat-Led Penetration Testing).
- **AI Act (EU)** — AI-specific risk audits become mandatory 2026-2027.
- **NATO/Ukraine Context** — Defense sector security spending growing aggressively.
- **NSM ProactiveCybersecurity** — National strategy driving security investment.

Potential Gaps in Market

1. SMB Segment

Mnemonic and KPMG target enterprise. SMBs (10-200 employees) are under-served and over-charged. Large gap for fixed-price pen-test packages.

2. AI/LLM Red-Team

Prompt injection, jailbreak testing, AI supply chain audit. Almost NO specialized firms in Norway. Greenfield opportunity 2026-2028.

3. DevSecOps Integration

Few firms offer continuous security testing vs. annual point-in-time pen-tests.

4. Balkan-Language Security Support

Niche: Norwegian firms with Balkan operations (raw materials, IT outsource) need Bosnian/Serbian-language security support.

⚠ **This is general industry knowledge** — NOT tool-verified ALAI market intelligence. For authoritative market data, consult NSM yearly threat assessment (nsm.no), Cybersecurity Norway market reports, IKT-Norge security working group.

Related: Security Certifications, Outsource Models

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

Outsource Models — Referral / White-label / Managed Service

Outsource Models — Referral / White-label / Managed Service

Context: If ALAI outsources pen-test work to a certified partner (partner holds CREST/NSM license, ALAI operates under it), there are three business models. **Recommended: Model 2 (White-label Sub-Kontrakt).**

Model 1: Referral (Easiest, Lowest Revenue)

How It Works

ALAI refers client to partner. Partner contracts directly with end-client.

What You Need

- Referral Agreement with partner
- Finder's fee: 10-25% of contract value

Risk

Low — ALAI not liable for technical delivery.

Marketing

"ALAI partners with [X]." You CANNOT claim partner's security work as your own.

Model 2: White-label Sub-Kontrakt (RECOMMENDED)

How It Works

ALAI signs prime contract with end-client. Partner performs technical work under sub-contract. ALAI is legal counterparty to client.

Margin

15-30% markup on partner's cost.

Legal Requirements

1. **Master Services Agreement (MSA)** with partner — back-to-back clauses
2. **Sub-Processor DPA (GDPR Art.28)** — partner processes client data
3. **NDA chain** — partner signs client-equivalent NDA
4. **Right-to-audit clause** over partner
5. **Cyber liability insurance back-to-back** — partner must carry minimum equivalent coverage to ALAI policy
6. **IP clause** — ALAI owns report to client; partner retains methodology IP
7. **SLA back-to-back** — whatever ALAI promises client, partner must promise ALAI
8. **Partner-cert legitimacy clause** — partner guarantees active CREST/NSM/PCI status during engagement

Norwegian Context

⚠ **Arbeidsmiljøloven §14-12 / §14-13 ("innleie")** — If partner sends individual testers (not a firm-to-firm service), it may be classified as employment leasing. Must structure as B2B firm-to-firm contract.

Marketing

- ✅ "Delivered in partnership with [X]"
- ✅ "Powered by [X]"
- ❌ "ALAI is CREST-certified" (false — partner is, ALAI is not)

Model 3: Managed Service (Most Complex, Highest Revenue)

How It Works

Subscription model. Recurring billing. ALAI provides customer success layer + partner provides technical delivery.

What You Need

- Everything from Model 2
- Customer success team on ALAI side
- Escalation matrix between ALAI and partner

What ALAI Holding Must Have (All Models)

1. ISO 27001 or plan to obtain (clients ask)
2. Cyber liability insurance 5-10M NOK (Gjensidige/IF) — see MC #9412
3. DPA template — □ already exists (AI Services legal pack)
4. MSA template — ⚠ NEED to add (similar to Retainer template)
5. Brønnøysund registration "konsulentvirksomhet sikkerhet" — already covered under existing NACE 62.02

Related: Legal & Marketing Constraints, Practical First Steps

Source: MC #10446, CEO email 2026-05-01 (Message-ID 4929b145)

Legal & Marketing Constraints When Outsourcing Security

Legal & Marketing Constraints When Outsourcing Security

⚠ **DISCLAIMER:** This is general industry knowledge. For authoritative legal advice, consult Norwegian advokat (Wiersholm/BAHR/Schjødt security practice) before signing any MSA or sub-contract.

Legal Requirements (White-label Model)

1. Master Services Agreement (MSA) with Partner

Back-to-back clauses — every obligation ALAI accepts from client must flow through to partner.

2. Sub-Processor DPA (GDPR Art.28)

Partner processes client personal data → must sign Sub-Processor Data Processing Agreement under GDPR Article 28.

3. NDA Chain

Partner must sign client-equivalent NDA. If client requires special classification (e.g., NSM Fortrolig), partner must hold equivalent clearance.

4. Right-to-Audit Clause

ALAI must have contractual right to audit partner's security practices. If partner refuses this clause → RED FLAG.

5. Cyber Liability Insurance Back-to-Back

Partner must carry cyber liability insurance coverage equivalent to ALAI's policy (minimum 5-10M NOK). ALAI must verify partner's insurance certificate annually.

6. IP Clause

- ALAI owns final report delivered to client
- Partner retains methodology and tooling IP

7. SLA Back-to-Back

If ALAI promises client "final report within 10 business days", partner must contractually promise ALAI "draft report within 7 business days".

8. Partner-Cert Legitimacy Clause

Partner guarantees active CREST/NSM/PCI certification during engagement period. If certification lapses, ALAI has termination right.

Norwegian Employment Law Constraint

Arbeidsmiljøloven §14-12 / §14-13 ("Innleie")

If partner sends individual testers to work under ALAI's direction (vs. partner delivering service as independent firm), Norwegian law may classify this as employment leasing.

Mitigation: Structure contract as firm-to-firm B2B service delivery. Partner retains operational control over testers. ALAI engages partner for deliverable (pen-test report), NOT for staff augmentation.

Marketing Do's and Don'ts

? Permitted Claims

- "Delivered in partnership with [X]"
- "Powered by [X]"
- "ALAI coordinates security testing through certified partners"

? Prohibited Claims

- "ALAI is CREST-certified" (false — partner is, ALAI is not)
- "ALAI is NSM Sikkerhetsgodkjent" (false — unless ALAI itself holds clearance)
- "ALAI performs pen-tests" (technically partner performs, ALAI coordinates)

?? Special Constraints for Specific Certifications

NSM Sikkerhetsgodkjent Work (Classified)

Only certified firms can deliver classified security work. ALAI CANNOT promise this unless ALAI itself obtains NSM clearance (12-24 month process).

PCI ASV Scan

Payment Card Industry Approved Scanning Vendor (ASV) reports must be signed directly by ASV firm. ALAI cannot white-label PCI ASV scans — client must contract ASV directly (or ALAI refers under Model 1).

What You CANNOT Promise to Client

- NSM Sikkerhetsgodkjent delivery (unless ALAI holds clearance)
- PCI ASV scan under ALAI name (ASV firm must sign report)
- Specific tester by name (partner retains operational control)

Related: Outsource Models, Practical First Steps

Source: MC #10446, CEO email 2026-05-01 (Message-ID 4929b145)

Practical First Steps + Partner Selection Red Flags

Practical First Steps + Partner Selection Red Flags

5-Step Roadmap to Launch ALAI Security Audit Service Line

Step 1: Identify 2-3 Norwegian Partners with CREST + ISO 27001

Recommended candidates:

- Defendable
- Netsecurity
- Possibly Promon

Do NOT approach:

- Mnemonic — they only operate as prime contractor, will not sub-contract

Step 2: NDA + Confidential Teaser Exchange

Share ALAI AI Services offering (existing legal pack, client pipeline, vertical focus). Gauge partner interest in white-label arrangement.

Step 3: Negotiate MSA Template (ALAI Preferred)

Use ALAI's preferred MSA template (to be created — similar to Retainer template in AI Services legal pack). Include all clauses from Legal & Marketing Constraints page.

Step 4: Pilot with One Client

Run single pen-test engagement. Verify:

- Operational quality of partner deliverable
- SLA adherence (timeline, report quality)
- Back-to-back DPA flow
- Client satisfaction

Step 5: Public Marketing (Only After Pilot Success)

Launch "ALAI Security Audit" service line publicly. Add to website, outreach campaigns, AI Services pricing page.

Partner Selection Red Flags

⚠ **Do NOT proceed** if partner exhibits any of these:

1. Certification Lapsed

Verify CREST registry directly (https://www.crest-approved.org/member-companies/). Do NOT rely on partner's claim alone.

2. Cyber Insurance < 5M NOK

Request current insurance certificate. If partner carries less than 5M NOK professional indemnity + cyber liability → STOP.

3. Refuse Right-to-Audit

If partner refuses contractual right for ALAI to audit their security practices → RED FLAG. This is standard for sub-processor relationships.

4. Refuse Back-to-Back DPA

If partner refuses to sign Sub-Processor DPA under GDPR Art.28 → STOP. This is non-negotiable for any client data processing.

5. Silent Sub-Contracting

Partner sub-contracts to third tier without ALAI's written approval. MSA must include "no further sub-contracting without prior written consent" clause.

Cost Estimate for Outsource Model Launch

White-label model (recommended): 200-500K NOK

- MSA legal drafting + Norwegian advokat review: 50-100K NOK
- Partner search + NDA negotiations: 20-40K NOK
- Pilot setup (ALAI project management overhead): 80-150K NOK
- Marketing materials (website, pricing page): 30-50K NOK
- Cyber insurance upgrade (if needed): 20-60K NOK/year

Comparison to building own security firm: 5-8M NOK upfront (certification journey, senior hires, insurance, tooling).

Open Questions for CEO Decision

1. **Which 2-3 partners to approach first?** (Defendable, Netsecurity, other?)
2. **ISO 27001 certification lead time for ALAI Holding?** (12-18 months typical — do we start now or wait until first client commits?)
3. **Cyber insurance vendor confirmation?** (Gjensidige, IF, other? MC #9412 referenced but status unclear.)
4. **Norwegian advokat for MSA review?** (Wiersholm/BAHR/Schjødt security practice — which firm and contact?)
5. **AI/LLM red-team specialization?** (Should ALAI position as AI-security specialist vs. general pen-test coordinator?)

Related: Outsource Models, Legal & Marketing Constraints

Source: MC #10446, CEO email 2026-05-01 (Message-ID 4929b145)