Accredited Africa Training Institute for Capacity Development
Unit FO409, Hatfield Plaza · 1122 Burnett St, Hatfield 0028 · Pretoria, Gauteng · South Africa
Tel: +27 12 004 8389 · Mobile: +27 65 077 6310
Email: apply@aaticd.co.za · Website: www.aaticd.co.za

COURSE BROCHURE

Counterintelligence Investigations For Threat Identification And Neutralisation Training

Law, Military Science and Security / Sovereignty of the State

Unit Standard 117369 · NQF Level 6 · 40 Credits · 37 Days

COURSE OVERVIEW

This course equips learners with the skills to identify, investigate, and neutralise counterintelligence threats within an organisational context. Participants will learn to apply investigative techniques, analyse threat indicators, and implement countermeasures to protect sensitive information and assets.

Category	Law, Military Science and Security
Subfield	Sovereignty of the State
Unit Standard	117369
Accreditation	SAQA Accredited · NQF Level 6 · 40 Credits
Duration	37 days
Training Method	Online, On-Campus, In-House
Certificate	Issued via AATICD LMS — verifiable online

LEARNING OUTCOMES

- Apply counterintelligence investigative methodologies to identify potential threats.
- Analyse threat indicators and patterns to assess risk levels.
- Design and implement countermeasures to neutralise identified threats.
- Demonstrate proficiency in conducting interviews and gathering evidence.
- Evaluate the effectiveness of counterintelligence strategies and adjust as needed.
- Implement reporting and documentation procedures in line with legal and ethical standards.

WHO SHOULD ATTEND

- This course is designed for security managers, intelligence officers, investigators, and professionals responsible for protecting organisational information and assets from espionage and insider threats.

COURSE OUTLINE

Day 1: Introduction to Counterintelligence and the Legal Framework

- Overview of counterintelligence concepts.
- Historical context and current threats.
- SAQA unit standard 117369 alignment.
- Relevant South African legislation (e.g., Intelligence Services Act, NCA).
- Ethics and professionalism in counterintelligence.
- Roles of SAPS, SANDF, and private sector.

Day 2: The Intelligence Cycle and Threat Identification

- Phases of the intelligence cycle.
- Threat identification methodologies.
- Risk assessment frameworks.
- Case studies: real-world threat examples.
- Practical exercise: mapping a threat scenario.

Day 3: Sources of Intelligence and Collection Methods

- OSINT: tools and techniques.
- HUMINT: recruitment and handling.
- SIGINT and IMINT overview.
- Source reliability and credibility.
- Practical exercise: OSINT collection on a simulated target.

Day 4: Counterintelligence Investigations – Planning and Preparation

- Investigation planning process.
- Resource management.
- Legal warrants and authorisations.
- Documentation and case file management.
- Practical exercise: drafting an investigation plan.

Day 5: Surveillance and Counter-Surveillance Techniques

- Types of surveillance.
- Counter-surveillance tactics.
- Technical surveillance detection.
- Practical exercise: conducting a mobile surveillance operation.
- Report writing for surveillance.

Day 6: Interviewing and Elicitation Techniques

- Interview planning and questioning strategies.
- Elicitation methods (e.g., assumption, opinion, ignorance).
- Detecting deception: verbal and non-verbal cues.
- Practical exercise: elicitation role-play.
- Ethical boundaries in interviews.

Day 7: Insider Threat Detection and Mitigation

- Insider threat categories (malicious, negligent, compromised).
- Behavioural indicators and profiling.
- Technical monitoring (access logs, data exfiltration).

- Mitigation policies and employee awareness.
- Case study: insider threat incident analysis.

Day 8: Cyber Counterintelligence and Digital Forensics

- Cyber threat landscape.
- Digital forensics: acquisition, preservation, analysis.
- Network monitoring and intrusion detection.
- Cyber counterintelligence techniques.
- Practical exercise: analysing a phishing attack.

Day 9: Counterintelligence Analysis and Threat Assessment

- Analytical methodologies.
- Link analysis and visualisation.
- Threat assessment reports.
- Briefing skills.
- Practical exercise: producing a threat assessment from raw data.

Day 10: Deception and Disinformation in Counterintelligence

- Deception techniques (e.g., cover stories, false flags).
- Disinformation detection and verification.
- Counter-deception measures.
- Case studies: historical deception operations.
- Practical exercise: identifying disinformation in a scenario.

Day 11: Counterintelligence Operations in the Private Sector

- Corporate espionage threats.
- Intellectual property protection.
- Private-public partnerships.
- Security clearance and vetting.
- Case study: industrial espionage investigation.

Day 12: Legal Aspects – Evidence Handling and Court Proceedings

- Law of evidence: admissibility, relevance.
- Chain of custody procedures.
- Witness preparation and testimony.
- Practical exercise: mock court testimony.
- Legal pitfalls in investigations.

Day 13: Counterintelligence and National Security – Interagency Cooperation

- SSA, NIA, SAPS, SANDF roles.
- Interagency task forces.
- Information sharing protocols.
- Security classifications (confidential, secret, top secret).
- Practical exercise: interagency coordination scenario.

Day 14: Advanced Surveillance and Technical Operations

- Advanced surveillance tools.
- TSCM: bug sweeping and detection.
- Legal authorisations for technical ops.
- Practical exercise: TSCM sweep.

- Ethics of technical surveillance.

Day 15: Counterintelligence Risk Management and Security Planning

- Risk management frameworks.
- Security plan components.
- Physical security: access control, perimeters.
- Personnel security: vetting, briefings.
- Practical exercise: developing a security plan.

Day 16: Counterintelligence in the Digital Age – Social Media and Open Sources

- Social media intelligence (SOCMINT).
- Social engineering tactics.
- OPSEC and digital footprint reduction.
- Practical exercise: social media investigation.
- Ethical considerations in online collection.

Day 17: Counterintelligence Case Management and Reporting

- Case management systems.
- Report writing standards.
- Executive briefings.
- Practical exercise: writing a case report.
- Lessons learned documentation.

Day 18: Crisis Management and Counterintelligence in Emergencies

- Crisis management frameworks.
- Incident response plans.
- Communication during crises.
- Practical exercise: simulated counterintelligence crisis.
- After-action review.

Day 19: Capstone Exercise – Integrated Counterintelligence Investigation

- Scenario introduction and team assignments.
- Investigation phase: planning, collection.
- Analysis and assessment.
- Neutralisation recommendations.
- Final report and presentation.

Day 20: Course Review, Assessment, and Professional Development

- Key concepts review.
- Written assessment.
- Practical assessment (scenario-based).
- Feedback and debrief.
- Professional development resources.
- Certification and next steps.

ASSESSMENT & CERTIFICATION

Delegates are assessed through exercises and a final test. A mark of **50% or above** earns an **AATICD Certificate of Completion**, issued digitally with a unique verification code. This course carries **40 NQF credits** at **NQF Level 6**.

PRICING (PER DELEGATE, EX-VAT)

Delegates	Training Method	Price per Delegate	Total
1	Online	R 115,500.00	**R 115,500.00**
1	In-House	R 150,200.00	**R 150,200.00**
1	On-Campus (Pretoria)	R 173,200.00	**R 173,200.00**

UPCOMING SESSIONS

Start	End	Method	Venue
10 Aug 2026	29 Sep 2026	On-Campus	Pretoria, South Africa
11 Aug 2026	30 Sep 2026	On-Campus	Abu Dhabi, UAE
12 Aug 2026	01 Oct 2026	On-Campus	Durban, South Africa
12 Aug 2026	01 Oct 2026	On-Campus	Mauritius
13 Aug 2026	02 Oct 2026	On-Campus	Cape Town, South Africa
14 Aug 2026	05 Oct 2026	On-Campus	Dubai, UAE
17 Aug 2026	06 Oct 2026	On-Campus	Abu Dhabi, UAE
18 Aug 2026	07 Oct 2026	On-Campus	Durban, South Africa

Contact us if no suitable date is listed — on-demand sessions can be arranged for groups.

HOW TO GET A QUOTE OR APPLY

1. **Get an instant quotation online:** visit **www.aaticd.co.za**, open the page for this course (Unit Standard 117369) and click **Get A Quote / Apply**. Select your training method and number of delegates — your quotation is generated immediately and emailed to you with the course brochure attached.
2. **Apply by email:** send the course title, your preferred training method (Online, In-House or On-Campus Pretoria), the number of delegates and your preferred dates to **apply@aaticd.co.za** — our team will reply with a formal quotation.
3. **Apply by phone or WhatsApp:** call **+27 12 004 8389** or WhatsApp **+27 65 077 6310** and we will prepare your quotation and reserve your seats.
4. **Confirm your booking:** accept the quotation and settle the invoice. As soon as payment is confirmed your delegates are enrolled and receive their AATICD LMS login details by email, along with joining instructions for their chosen training method.

Group discounts apply automatically — the more delegates you enrol, the lower the price per delegate. No payment is required to request a quotation.

Accredited Africa Training Institute for Capacity Development
Unit FO409, Hatfield Plaza, 1122 Burnett St, Hatfield 0028, Pretoria, Gauteng, South Africa
Tel: +27 12 004 8389 · WhatsApp: +27 65 077 6310 · apply@aaticd.co.za · www.aaticd.co.za