Understanding the threat. Strengthening preparedness. Building resilience. Sustaining what matters.

SUMMARY

Industrial Security & Terrorism Preparedness (ISTP) is a management-level professional programme strengthening terrorism preparedness and resilience across complex industrial environments, critical infrastructure, organisations and communities. It is delivered jointly by Universitas Indonesia — with UI's Terrorism Studies Centre and School of Strategic and Global Studies (SKSG) as academic engines — INDOGUARD.org and 3S Sandi Satria Solo over **six days at the Universitas Indonesia campus in Salemba, with four-star hotel accommodation in Jakarta**: nine modules in two domains, five work products on the participant's organisation, and a capstone before an academic–practitioner panel.

Bridging Indonesian industrial realities with global perspectives on terrorism preparedness, security, resilience and sustainability.

Programme character: scholarship and analysis, pre-emptive and preventive — including surveillance & detection and early warning. ISTP is **not a combat course or tactical training**.

- **Cohort:** Pilot Cohort, 22–27 November 2026. A six-day on-site programme at the Universitas Indonesia campus in Salemba, Central Jakarta; participants stay at a four-star hotel in Jakarta (accommodation included). Hotel check-in Sunday 22 November 2026 at 14:00 WIB; closing Friday 27 November 2026 at 12:00 WIB.
- **Venue:** Universitas Indonesia campus, Salemba, Central Jakarta — the venue for all sessions; participants stay at a four-star hotel (accommodation included, the hotel is confirmed to registered participants)
- **Language of instruction:** Bahasa Indonesia and English (bilingual)
- **Capacity:** 20–30 participants
- **Fee:** IDR 20,000,000; pilot reduction IDR 3,000,000; payable **IDR 17,000,000** (≈ US$955), VAT 11% included, including four-star hotel accommodation and full board
- **Certificate:** Assessment-based Certificate of Achievement co-issued by UI · INDOGUARD.org · 3S (not a BNSP/SKKNI certification)

WHO SHOULD ATTEND

- **CSOs, Heads of Security & Security Managers**
- **Critical Infrastructure & National Vital Object Operators**
- **Senior Leaders of Security Service Companies**
- **Risk, Compliance, HSE & Business Continuity**
- **Property, Hospitality & Crowded-Place Managers**
- **Buyers of Security Services**
- **Gada Utama Holders in Leadership Roles**

CORE NARRATIVE

1

Terrorism Risk

Understand intent, capability and exposure in your operating context.

Modules: A1 · A2 · A4

2

Preparedness

Governance, risk ownership and reporting lines in place before they are needed.

Modules: B1 · B3

3

Security Resilience

Early warning, surveillance awareness and proportionate layered protection.

Modules: A2 · A3 · B2

4

Continuity

Critical functions maintained through disruption, then recovered with discipline.

Modules: B4

5

Sustainability

Organisations that protect people, assets and communities over the long term.

Modules: B5

CURRICULUM

MODULE	TITLE & FOCUS	WORK PRODUCT
A1	**The Terrorism Landscape and Industrial Targets** Building a research-based understanding of contemporary terrorist threats and why industrial environments become targets — grounded in evidence rather than perception or headlines.	Sector threat-landscape note
A2	**Modus Operandi, Targeting and Pre-Incident Indicators** Reading the attack-planning cycle analytically to find the earliest detection window — the core of a pre-emptive approach: recognising threats before they become incidents.	Pre-incident indicator matrix
A3	**Intelligence, OSINT and Early Warning** Applying the intelligence cycle in a corporate setting, lawfully and ethically, to build an accountable early-warning system.	Early-warning scheme design
A4	**Industrial Terrorism Threat Assessment Workshop** A guided workshop integrating A1–A3 into a structured threat assessment of the participant's own organisational assets and operations.	D1 — Threat Assessment
B1	**Governance and Enterprise Security Risk Management** Translating the threat assessment into a corporate risk profile with clear ownership, risk appetite and governance.	D2 — Security Risk Profile

MODULE	TITLE & FOCUS	WORK PRODUCT
B2	**Integrated Industrial Security Architecture** Designing integrated protection proportionate to risk — across physical, electronic, personnel, cyber and operational technology.	D3 — Security Improvement Plan
B3	**Security Economics, Stakeholders and Service-Provider Governance** Positioning security as an accountable business enabler for top management, from budget to service-provider performance.	Business-case framework and KPI/SLA framework
B4	**Crisis Command, Business Continuity and Resilience** Leading decisions under uncertainty and keeping critical operations running through recovery and organisational learning.	D4 — Crisis & Continuity Annex
B5	**Integrated Capstone — Executive Resilience Exercise** An integrated management-level exercise testing all six competencies at once through a single, integrated industrial scenario.	D5 — Dossier, Resilience Roadmap & Executive Briefing

GRADUATE COMPETENCIES

- **EC1 Threat & Intelligence** — Prepare a terrorism and emerging-threat assessment for an industrial asset or operation, complete with early-warning indicators and a stated level of confidence.
- **EC2 Security Risk & Governance** — Translate a threat assessment into a corporate security risk profile with criticality, risk ownership, risk appetite and defensible treatment options.
- **EC3 Industrial Protection Architecture** — Design an integrated protection architecture across physical, electronic, personnel, cyber and operational technology, using deter–detect–delay–respond logic with a proportionality case.
- **EC4 Security Economics & Stakeholder** — Build a security business case and budget, and steer stakeholders and security service providers through performance indicators and service-level agreements.
- **EC5 Crisis, Continuity & Resilience** — Lead crisis decisions under uncertainty and set continuity priorities for critical operations through recovery and organisational learning.
- **EC6 Executive Security Communication** — Present security recommendations to top management in the language of risk, business impact and investment decisions.

SIX-DAY JOURNEY

DAY	THEME
Day 1 · Sunday, 22 November 2026	Arrival, Orientation & Opening
Day 2 · Monday, 23 November 2026	Threat Landscape × Governance Foundations
Day 3 · Tuesday, 24 November 2026	Intelligence × Protection Architecture
Day 4 · Wednesday, 25 November 2026	Risk × Protection × Security Economics
Day 5 · Thursday, 26 November 2026	Improvement Planning, Crisis & Detection Exercise
Day 6 · Friday, 27 November 2026	Capstone & Closing

HOW TO REGISTER

1

Register & upload your CV

Complete the registration form, upload your CV (PDF) and tick the statement of interest. You immediately receive an email with your registration number.

2

Selection & background check

Reviewed together with Universitas Indonesia within 3 working days. No payment is made at this stage.

3

Seat Confirmation Letter

If selected, you receive the official programme account and a personal link to upload your proof of payment. Payment deadline: 7 days, with a reminder 2 days before.

4

Payment & verification

Transfer to the official Universitas Indonesia account and upload your proof via your personal link. Funds are verified within 2 working days.

5

Welcome to ISTP

Your official INDOGUARD account, ISTP Room, digital badge, digital receipt from the ISTP Programme Office and programme guide are sent to your email.

INCLUDED

- A six-day residential programme: lectures, workshops, academic–practitioner dialogue blocks, simulation exercises and a capstone
- Four-star hotel accommodation in Jakarta for the residential period
- Full board throughout the programme: breakfast, lunch, dinner and coffee breaks
- Course materials, participant workbook and pre-programme materials
- Assessment of work products, written feedback and panel assessment
- Certificate of Achievement co-issued by Universitas Indonesia, INDOGUARD.org and 3S Sandi Satria Solo for participants who meet the pass standard
- Personal accident insurance during programme activities

Not included: travel to and from your home city and to the hotel; personal hotel expenses (laundry, minibar, room service) and extra nights outside the programme period.

CANCELLATION POLICY

SITUATION	TERMS
Cohort cancelled or postponed by the organisers (including where the minimum of 20 participants is not reached)	100% refund, or transfer to the next cohort at the participant's choice

SITUATION	TERMS
Participant cancels 30 calendar days or more before Day 1	90% refund (10% administrative fee)
Participant cancels 14–29 calendar days before Day 1	50% refund, or one free transfer to the next cohort
Participant cancels less than 14 calendar days before Day 1, or does not attend	No refund; transfer to the next cohort with a 10% administrative fee, or substitution by another participant
Participant substitution	Free of charge until 3 working days before Day 1, with complete details of the substitute

CONTACT

Registration: academy@istp.online · Partnership: partnership@istp.online · General: hello@istp.online · WhatsApp +62 896-2927-1196 · Gedung Mochtar, Jl. Pegangsaan Timur No. 16 Lt. 2, Pegangsaan, Menteng, Jakarta Pusat 10320 · istp.online

Curriculum Revision 1.1 · six-day residential format · effective 10 October 2026. US$ equivalents are indicative at IDR 17,800 per US$1. All invoicing and payment is in IDR. Participant payments are received in the official Universitas Indonesia account. VAT (11%) is remitted through the tax account of the Pranata Pembangunan Research Centre, School of Sustainable Development, Universitas Indonesia (NPWP 02.486.770.7-412.000), under the ISTP cooperation agreement.