Australian Institute
of Insider Threats

INSIDER THREAT PROGRAM

Expert Certificate

COURSE GUIDE

ABOUT THE PROGRAM

The **Insider Threat Program Expert** is AIIT's most advanced professional program, designed for experienced practitioners who are ready to move beyond operating insider threat activities and into assessing, shaping, and leading insider threat capability at an enterprise level.

This program is built on a hard but often overlooked reality: Most insider threat failures are not caused by missing tools, policies, or technology. They are caused by poor judgement under uncertainty, weak maturity assessment, and an inability to advise leaders clearly when trade-offs are unavoidable.

Over 10 weeks, participants operate inside a single evolving organisational scenario that mirrors real life. Information is incomplete. Signals are ambiguous. Stakeholders disagree. Third-party dependencies and AI-enabled systems introduce risk beyond organisational boundaries.

Decisions made early in the program have consequences later, forcing participants to think systemically rather than tactically.

☑ **10-WEEK ADVANCED PROFESSIONAL PROGRAM**

☑ **WEEKLY 2-HOUR LIVE VIRTUAL SESSIONS**

☑ **IN-PERSON CAPSTONE**

☑ **CERTIFICATE OF COMPLETION – INSIDER THREAT PROGRAM EXPERT**

WHO THIS PROGRAM IS FOR

This program is designed for experienced professionals who already understand insider threat fundamentals and operations, and who are now expected to advise, influence, or lead at a higher level.

It is particularly suited to:

- Insider Threat Program Managers and Leads
- Security, Cybersecurity, and Risk Leaders
- HR, Legal, Compliance, and Governance professionals supporting insider risk
- Behavioural risk, integrity, and fraud specialists
- Senior practitioners preparing to brief executives or boards
- Professionals progressing toward Trainer or enterprise leadership roles

Prerequisite: Completion of the Insider Threat Program Professional (or equivalent experience, subject to AIIT approval).

LEARNING OBJECTIVES

By the end of this program, participants will be able to:

- Assess insider threat program maturity using structured, evidence-based models
- Diagnose systemic organisational weaknesses that amplify insider risk over time
- Design realistic, risk-based uplift strategies aligned to organisational constraints
- Apply ethical, privacy, and trust principles in ambiguous, high-pressure situations
- Address insider risk involving third parties, contractors, privileged administrators, and AI-enabled systems
- Translate insider threat risk into clear, executive- and board-level language
- Defend decisions using recognised frameworks, metrics, and professional judgement

TOPICS COVERED

- Insider threat capability architecture and common failure modes
- Program maturity assessment and auditability
- Alignment to the SEI Common Sense Guide (22 practices)
- AIIT Insider Resilience Framework mapping
- Behavioural and technical detection at scale
- Signal vs noise, bias, and false positives
- Strategic uplift planning and prioritisation
- Third-party, contractor, and privileged access risk
- Ethical decision-making and lawful monitoring
- Governance, oversight, and executive reporting
- Crisis response, consequence management, and recovery
- Leader enablement, incentives, and speak-up culture

BENEFITS OF THE PROGRAM

Participants who complete the Insider Threat Program Expert gain:

Expert-Level Confidence:
The ability to assess insider threat capability, challenge assumptions, and advise senior leaders without relying on tools, templates, or hindsight.

Defensible Professional Authority
Clear, structured reasoning aligned to recognised best practice, enabling confident defence of decisions to executives, boards, regulators, or auditors.

Reusable Practical Artefacts
Participants leave with artefacts they can reuse immediately, including maturity assessments, SEI crosswalks, framework mappings, KPI dashboards, executive briefings, and decision rationale templates.

Real-World Readiness
Experience dealing with insider risk as it actually unfolds - slowly, ambiguously, and across organisational boundaries, not as a one-off exercise.

COURSE STRUCTURE & TOPICS

- **Duration:** 10 weeks
- **Delivery:** Weekly 2-hour live virtual sessions
- **Learning Model:** Longitudinal scenario with individual and group work
- **Assessment:** Continuous, based on judgement, evidence, and decision defence
- **Capstone:** In-person, multi-day expert capstone experience
- **Certification:** Certificate of Completion – Insider Threat Program Expert

WEEK 1 EXPERT MINDSET & BASELINE REALITY

Participants transition from operational thinking to expert-level judgement.

This week establishes how insider threat risk emerges from systems, culture, and decisions, not just incidents.

Learners assess the baseline reality of the organisation, identify early risk signals, and practise restraint by deciding what not to act on yet.

WEEK 2 PROGRAM MATURITY & ALIGNMENT

Participants learn how to assess insider threat capability using evidence rather than assumptions.

This week introduces structured maturity assessment, alignment to the SEI Common Sense Guide, and mapping to the AIIT Insider Resilience Framework, creating an audit-ready view of the program's true state.

WEEK 3 DIAGNOSING SYSTEMIC WEAKNESS

This week moves beyond individual events to uncover systemic drivers of insider risk.

Participants analyse organisational patterns, cultural blind spots, and governance weaknesses that quietly amplify insider threat over time, learning how to distinguish root causes from surface symptoms.

WEEK 4 DETECTION, NOISE & BIAS

Participants develop expert discernment in interpreting behavioural and technical signals.

This week focuses on separating meaningful indicators from noise, managing false positives, recognising analytic bias, and understanding when action may create more risk than it resolves.

WEEK 5 STRATEGIC UPLIFT & DEPENDENCIES

Learners prioritise insider threat uplift actions within real-world constraints.

The focus shifts to dependencies such as third-party providers, contractors, and privileged administrators, forcing participants to confront risk they do not fully control and make defensible trade-off decisions.

WEEK 6

ETHICS, PRIVACY & TRUST AT SCALE

This week challenges participants to navigate ethical grey zones where lawful action may still undermine trust.

Learners balance privacy, proportionality, and risk while responding to sensitive scenarios such as whistleblower reports, monitoring decisions, and shared-service limitations.

WEEK 7

EXECUTIVE & BOARD ADVISORY

Participants translate technical and behavioural insight into executive-level communication.

This week builds confidence in briefing leaders, framing uncertainty, explaining residual risk, and defending decisions under challenge, without alarmism or false reassurance.

WEEK 8

CRISIS & CONSEQUENCE

Earlier decisions come due as the scenario escalates into a high-pressure incident.

Participants lead response efforts, manage escalation, coordinate stakeholders, and experience the real consequences of earlier choices - both good and bad.

WEEK 9

REASSESSMENT & CAPSTONE PREPARATION

Learners reassess program maturity in light of the incident, consolidate lessons learned, and refine their narrative.

This week focuses on preparing a coherent, evidence-based defence for the final capstone, including maturity movement, trade-offs, and outcomes.

WEEK 10

IN-PERSON CAPSTONE: ASSESS, DECIDE, DEFEND

The program culminates in a 3-day in-person capstone.

Participants respond to a live, evolving insider threat scenario, defend decisions before an executive-style panel, complete a mini-lab on third-party and AI-enabled risk, design leader enablement and speak-up safety interventions, and conclude with a structured capstone debrief that consolidates professional judgement.

Australian Institute
of Insider Threats

INSIDER THREAT PROGRAM

Expert Certificate

COURSE GUIDE

CONTACT US

✉ hello@insider threats.com. au

🌐 www.insiderthreats.com.au