



Australian Institute
of Insider Threats

ESTABLISHING AN INSIDER THREAT PROGRAM IN 90 DAYS

PROGRAM GUIDE

PROGRAM OVERVIEW

Most organisations understand the importance of insider threat management, but few know how to actually build a program that works.

Establishing an Insider Threat Program in 90 Days is the Australian Institute of Insider Threats (AIIT) flagship live program, designed to give security, risk, HR, compliance and insider threat professionals a clear, structured, and supported pathway to design an organisation-wide insider threat capability.

This program is not theory-based training. It is a hands-on, guided implementation program that walks you step-by-step through designing your organisation's Insider Threat Program, from governance, to monitoring, to awareness, to response planning.

By the end of the 10 weeks, you will have a **complete, executive-ready 90-day Insider Threat Program Roadmap** tailored to your organisation. A practical plan of attack you can begin implementing immediately.

INCLUDED FREE

INSIDER THREAT FOUNDATIONS COURSE (WEEKS 1–2)

When you enrol, you receive instant access to the full 6-hour AIIT Insider Threat Foundations Course at no additional cost.

This provides the essential baseline knowledge every participant must have before beginning the live cohort sessions.

The Foundations Course covers:

- Insider threat definitions and categories
- Behavioural and technical indicators
- Insider motivations
- Negligent vs malicious vs compromised insiders
- Organisational blind spots
- Case studies and lessons

This ensures that all participants enter Week 3 prepared, aligned and confident.

PROGRAM STRUCTURE:

10 WEEKS
TOTAL

WEEKS 1–2: INSIDER THREAT FOUNDATIONS LIVE

The program begins with a **two-week live Foundations module** designed to rapidly build the essential knowledge you need before constructing an Insider Threat Program.

Across two highly focused 3-hour sessions, we strengthen your understanding of:

- What insider threat really is (and isn't)
- How insider incidents manifest across organisations
- The different types of insiders (negligent, malicious, compromised, colluding)
- Motivations and behavioural drivers
- Early warning indicators and red flags
- The organisational blind spots that increase risk
- Real-world case studies and lessons
- The difference between insider threat capability vs insider threat events

This live Foundations module ensures all participants begin Week 3 with:

- A common language
- A shared baseline of insider threat knowledge
- Confidence in the underlying concepts
- A mature understanding of behaviours, risks, and patterns
- The grounding required to build a program responsibly

Note: There is no program-building in Weeks 1–2. Only essential foundational learning. Once these foundations are in place, the remaining 8 weeks focus entirely on implementation, design, and capability-building.

WEEK BREAKDOWN

Each week includes a 90-minute live session, downloadable templates, and structured tasks.

WEEK 3 – DISCOVERY & CURRENT STATE MAPPING

Gain a clear, honest picture of your organisation's current insider threat maturity. This week uncovers the gaps, blind spots, strengths, and existing controls that will shape your 90-day program.

Output: Current State Map + Gap Summary

WEEK 4 – EXECUTIVE ALIGNMENT & INSIDER THREAT CHARTER

Learn how to engage senior leaders and secure the mandate required to build your program effectively. You will define the program's purpose, scope and boundaries, and craft the messaging that gets executive buy-in.

Output: Executive Mandate + Draft Charter

WEEK 5 – CROWN JEWELS, HIGH-RISK ROLES & INSIDER PERSONAS

Identify what matters most and who poses the highest risk to those assets. This week enables you to prioritise focus areas based on value, access, exposure and organisational risk appetite.

Output: Crown Jewels Inventory + Persona List

WEEK BREAKDOWN

Each week includes a 90-minute live session, downloadable templates, and structured tasks.

WEEK 6 – GOVERNANCE, ROLES & OPERATING MODEL

Design the structure that makes your insider threat capability sustainable. You will define responsibilities, establish cross-functional governance, and build a practical operating model that aligns with your organisation.

Output: Governance Framework + RACI Matrix

WEEK 7 – MONITORING, DATA SOURCES & DETECTION ARCHITECTURE

Learn how to develop a realistic, scalable monitoring approach based on your current tools and risk profile. You will map available data sources, determine detection priorities, and create a monitoring strategy you can implement immediately.

Output: Monitoring & Detection Map

WEEK 8 – RESPONSE PROCESSES & THE FIRST 48 HOURS PLAYBOOK

Build a clear, repeatable response workflow for managing insider incidents. This week equips you with triage criteria, escalation pathways, and a proven First 48 Hours Playbook for rapid, coordinated action.

Output: Insider Threat Management Playbook

WEEK BREAKDOWN

Each week includes a 90-minute live session, downloadable templates, and structured tasks.

WEEK 9 – AWARENESS, TRAINING & CULTURAL INTEGRATION

Create a practical awareness and behavioural culture plan that supports early detection and safe reporting. You will develop targeted messaging, lifecycle touchpoints, and engagement strategies to embed insider threat into everyday operations.

Output: Awareness & Culture Plan

WEEK 10 – METRICS, REPORTING & FINAL 90-DAY PROGRAM

Bring all components together into an executive-ready program you can confidently deliver. You will establish KPIs, dashboards, maturity indicators, and finalise a comprehensive 90-day rollout plan tailored to your organisation.

Output: Complete Executive-Ready 90-Day Insider Threat Program

WHAT YOU WILL HAVE BY THE END

During this 10-week program, you will not be building your insider threat capability — you will be designing it.

You will walk away with a complete, organisation-specific **90-day Insider Threat Program Roadmap**, including:

- A tailored plan of attack for establishing your Insider Threat Program
- A draft insider threat governance framework
- A Crown Jewels Asset Inventory
- A monitoring & detection blueprint
- A draft Insider Threat Management Playbook
- A practical awareness & culture plan
- A KPI and executive reporting dashboard
- Certificate of Completion for both the Insider Threat Foundation and Building an Insider Threat program in 90 Days.

This roadmap provides a clear, structured and realistic 12-week implementation plan you can begin immediately after the program.

WHO THIS PROGRAM IS FOR

This program is ideal for:

- Security Managers
- Insider Threat Professionals
- Cybersecurity Management/Leaders
- Risk Professionals
- GRC Teams
- Protective Security Professionals
- Business Continuity/Crisis Leaders

INCLUDED RESOURCES

Participants receive:

- Insider Threat Foundations Course **(FREE)**
- Access to AIIT Membership
 - AIIT Digital Mind AI Avatar
 - All templates and planning tools
 - Governance & policy templates
 - Crown Jewels Assessment tool
 - Persona worksheets
 - Monitoring & data mapping tool
 - Response playbooks
 - Awareness materials
 - KPI/dashboard templates

KEY VALUE

In just 10 weeks, you will leave with a complete, executive-ready roadmap to establish your Insider Threat Program within 90 days — Practical, structured, tailored and ready for immediate implementation.



Australian Institute
of Insider Threats

ESTABLISHING AN INSIDER THREAT PROGRAM IN 90 DAYS

PROGRAM GUIDE

CONTACT US



hello@insiderthreats.com.au



www.insiderthreats.com.au