ALLIED UNIVERSAL®

There for you.

# 7 Step Guide to Insider Threat Management

## Building a Team that Fortifies Organizations Against Internal Risks

aus.com

# Introduction

Insider threats represent one of the most complex and potentially damaging risks that private enterprises are exposed to. Unlike external adversaries, insiders—whether acting maliciously, negligently, or under duress—already have legitimate access to systems, data, and facilities. This access makes them uniquely capable of bypassing traditional security controls, often remaining undetected until significant harm has occurred.

An effective insider threat mitigation strategy requires a deliberate, structured approach that integrates physical security, cybersecurity, HR, legal, and operational expertise. At the center of this strategy is the Insider Threat Management Team (ITMT)—a cross-functional group empowered to identify, assess, and respond to insider risks in a coordinated and legally defensible manner.

A well-designed ITMT enables organizations to reduce the likelihood and impact of insider threats while fostering resilience, trust, and accountability across the enterprise.

# Step 1: Establish Executive Sponsorship and Governance

To succeed, insider threat programs should be grounded in organizational authority and supported with appropriate resources. Executive sponsorship ensures strategic alignment with enterprise risk management goals and grants the program legitimacy across departments. Without this backing, initiatives risk stalling due to lack of priority or interdepartmental friction.

To build executive support:

- Present a compelling business case using relevant industry incidents and cost implications (ie. data theft, sabotage, workplace violence, or counterfeit).
- Align the program with the organization's risk appetite and regulatory obligations (i.e. SOX, HIPAA, CMMC).
- Determine whether the ITMT will be overseen by a single executive or a broader risk committee.

# Step 2: Assemble a Multidisciplinary Team

Insider threats extend beyond the domain of security alone. They affect digital infrastructure, workplace behavior, regulatory compliance, and facility access. A successful ITMT brings together diverse stakeholders to ensure holistic risk detection, intervention, and response.

Core team members might include:

- Physical Security: To identify and mitigate threats to physical assets.
- IT / Cybersecurity: To analyze and mitigate digital vulnerabilities.
- Human Resources/Employee Assistance: To advise on employment practices and behavior management.
- Legal / Compliance: To ensure alignment with laws, policies, and contracts.
- Facilities / Operations: For physical access and security controls.

# Step 3: Define Mission, Scope and Objectives

A clearly defined mission ensures that all stakeholders understand the ITMT's purpose, responsibilities, and limitations. This foundation sets the direction for resource planning, engagement strategy, and program boundaries—preventing scope creep and misaligned expectations.

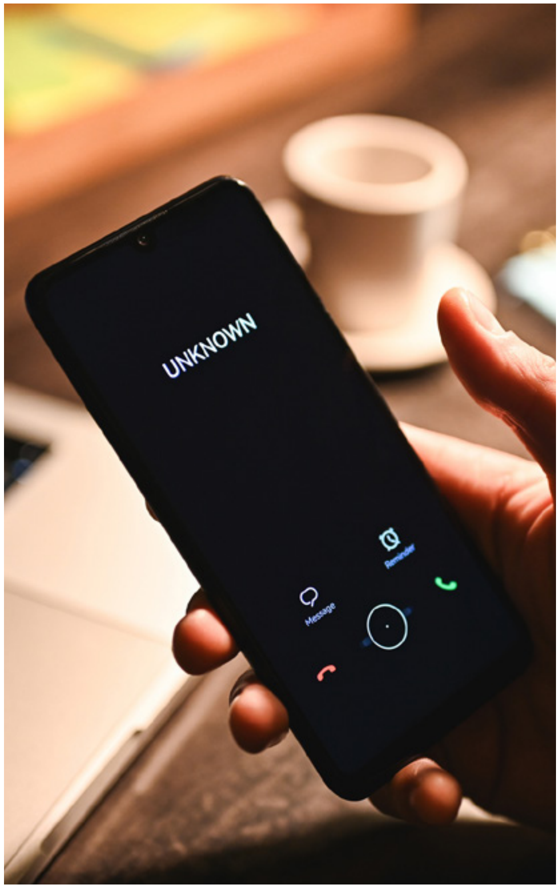
- Define the scope to determine team focus on cyber, physical, behavioral threats—or a combination of these.
- Clarify what constitutes an insider threat within your organization (i.e. malicious actors, negligent users, compromised individuals).
- Craft a mission statement to guide activity similar to below.
  "*To proactively detect, deter, and mitigate threats from individuals with authorized access to enterprise systems, data, or facilities.*"

# Step 4: Develop Policies, Protocols, and Legal Frameworks

Policy provides the framework for consistent enforcement, employee guidance, and legal defensibility. It also clarifies what constitutes a violation and how investigations and responses will be conducted.

- Define reportable behaviors and establish formal reporting procedures.
- Set policies for acceptable use, data monitoring, and access controls.
- Outline disciplinary actions for violations and the process for escalation.
- Involve legal counsel to ensure compliance with privacy laws, union agreements, and industry regulations.

# Step 5: Implement Detection and Response Protocols



Detection and response form the operational heart of insider threat management. Detection tools identify early indicators of risk, while response protocols ensure that incidents are managed consistently, lawfully, and effectively.

Detection methods may include:

- Behavioral: Monitoring stressors or anomalies identified by HR, EAP or management reporting.
- Physical: Analyzing badge activity and security video footage.
- Technical: Using UEBA (User and Entity Behavior Analytics), DLP (Data Loss Prevention), and SIEM (Security Information and Event Management).

Response protocols might include:

- Tiered actions: based on severity, will respond by monitoring, investigating, or intervening.
- Escalation paths: respond with clearly defined escalation paths and documentation standards.
- Integrated approach: respond by integrating with legal and HR processes to maintain procedural fairness.

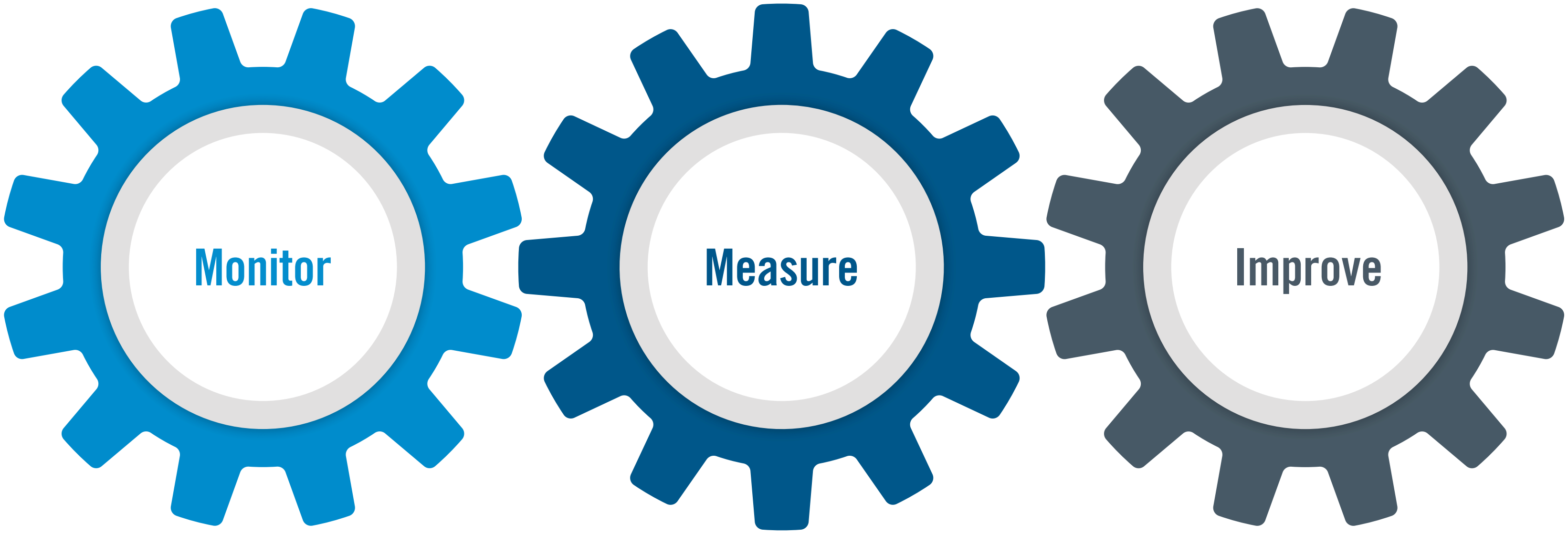
# Step 6: Train and Communicate

Training and communication foster a culture of awareness and accountability. Employees and managers need to understand the ITMT's purpose, how to report concerns, and what protections are in place to ensure confidentiality and due process.

- Deliver annual training for all employees and integrate it into onboarding programs.
- Provide specialized training for managers on identifying and reporting risk indicators.
- Develop internal messaging that reinforces the program's objectives and builds trust.

# Step 7: Turn Data Into Action

Effective programs evolve. Establishing metrics and feedback mechanisms ensures the ITMT remains aligned with emerging risks and business needs. Post-incident reviews help uncover systemic gaps and guide continuous improvement.

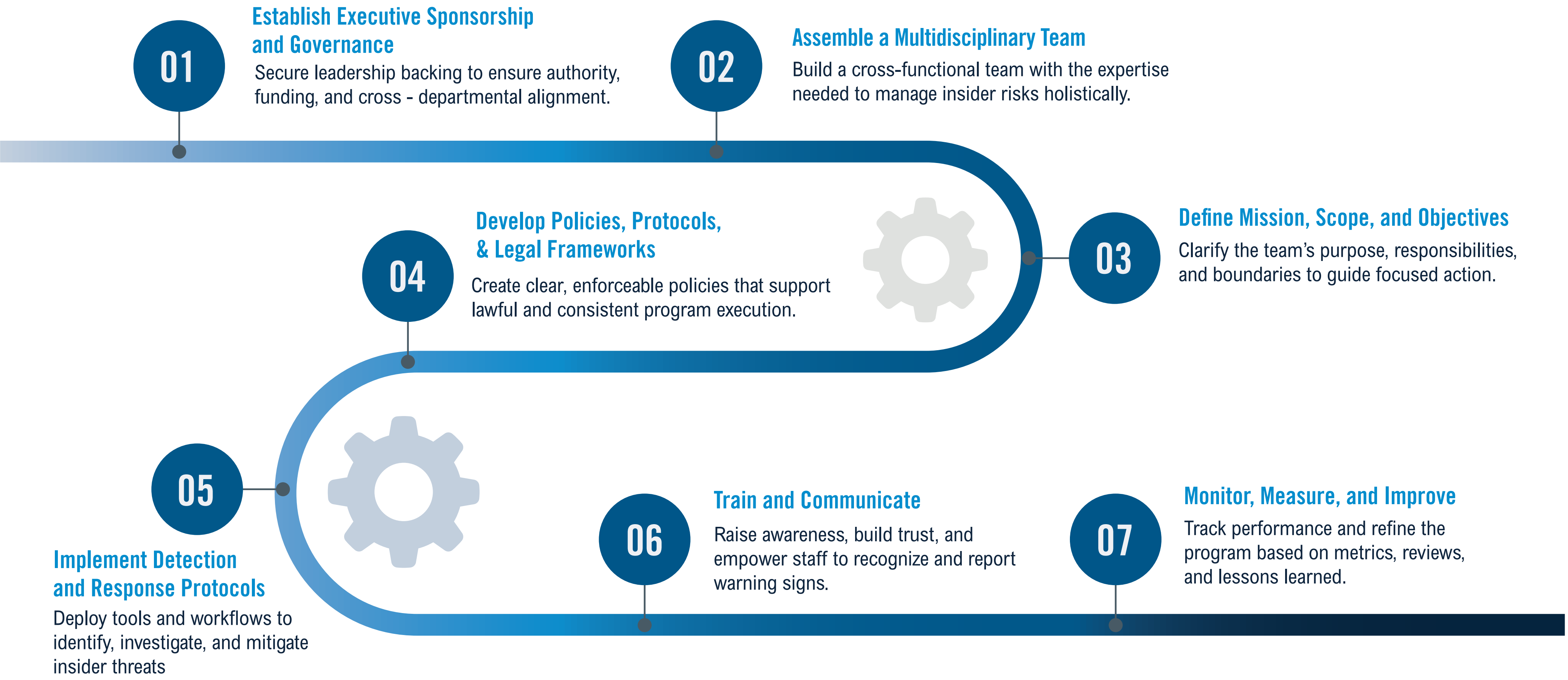


Track key performance indicators (i.e. time to resolution, number of cases, incident trends).

Conduct periodic risk assessments, policy reviews, and control audits.

Analyze incidents to extract lessons learned and identify recurring vulnerabilities.

# Insider Threat Management Team Creation Process



01

### Establish Executive Sponsorship and Governance

Secure leadership backing to ensure authority, funding, and cross - departmental alignment.

02

### Assemble a Multidisciplinary Team

Build a cross-functional team with the expertise needed to manage insider risks holistically.

03

### Define Mission, Scope, and Objectives

Clarify the team's purpose, responsibilities, and boundaries to guide focused action.

04

### Develop Policies, Protocols, & Legal Frameworks

Create clear, enforceable policies that support lawful and consistent program execution.

05

### Implement Detection and Response Protocols

Deploy tools and workflows to identify, investigate, and mitigate insider threats

06

### Train and Communicate

Raise awareness, build trust, and empower staff to recognize and report warning signs.

07

### Monitor, Measure, and Improve

Track performance and refine the program based on metrics, reviews, and lessons learned.

# Conclusion

Insider threats remain one of the most underestimated and potentially damaging risks facing modern organizations. Forming an Insider Threat Management Team (ITMT) is a strategic step toward proactive risk governance. The ITMT serves as the central hub for early detection, coordinated response, and long-term organizational resilience.

But success requires more than structure—it demands insight, experience, and adaptability. Allied Universal's Risk and Vulnerability Consulting Services can support your ITMT development with:

- Comprehensive vulnerability assessments
- Integrated insider threat mitigation and response strategies
- Ongoing evaluation for continuous improvement and compliance

Allied Universal provides the strategic guidance and operational expertise to help make your insider threat initiative successful, sustainable, and defensible.

**Learn more about Allied Universal Risk and Vulnerability Consulting Services:**
https://www.aus.com/security-services/enhanced-protection-services/risk-and-vulnerability-consulting

ALLIED UNIVERSAL®
There for you.

# 7 Step Guide to Insider Threat Management

Learn more about Allied Universal by visiting our website - aus.com - and exploring additional resources, tools, and insights.

Guarding

Integrated Technology

Risk and Vulnerability Consulting

Canine Security

Executive Protection and Intelligence

Active Law Enforcement

Weapons and Explosive Screening

Event Security

Investigations

Disaster and Emergency Response

Electronic Monitoring

Cash Solutions

Workforce Solutions

Janitorial Services

There's Security in our Solutions®