How to Run Effective Insider Risk Investigations

Protecting employees, assets, and intellectual property against the negligent, accidental, and malicious actions of insiders is a priority for organizations. With the right tools and processes in place, you can recognize potential risk indicators, take proactive action, streamline investigations, and gain insights to support your insider risk program.

Leverage the following checklist to ensure you have a comprehensive investigative process in place.

Pre-Incident

Establish systems and processes

Ensure you have the right tools in place to proactively screen and monitor for insider incidents and establish processes to mitigate risks, reduce response times, and create standardization in an investigation workflow across the team.

Conduct a risk assessment to define critical assets for protection This could include sensitive or protected data, intellectual property (IP), credentials, corporate devices, systems, secure facilities, or high value individuals	☐
Map information sources and resources Including individual team sources, disparate information streams, and intelligence capabilities	☐
Consolidate connected systems data From sources like license plate readers, visitor management systems (VMS), access control, CRM, case management (past and current), and legacy systems	☐
Centralize research and monitoring tools Including criminal and civil records, OSINT, social media, dark web, local news reports, and localized crime data	☐
Review and update insider risk programs and policies Including pre-employment background checks, continuous review cycles, post-termination monitoring, trigger points, escalation paths, and privacy controls	☐
Define tripwires This could include grievances (internal and external), lawsuits, terminations, policy violations, disengaged employees, reported disruptive or concerning behavior, unusual visitor requests, unusual physical or digital access requests, or negative online commentary	☐
Set up notification flows based on threat type or urgency level Consider including corporate security, HR, legal, third-party experts, PR, and local law enforcement	☐

Continued on next page

Establish reporting protocols If not through the Insider Risk Working Group, how are issues documented, reported, and (if necessary) briefed to decision makers?	☐
Select conditions for report status or closure and length of storage Like inactive, referred to police, risk mitigated, and unresolved (most report closures will be 'soft' based on the information at the time of closure)	☐

Monitor and identify potential concerns

By establishing situational awareness based on systems and tools, teams can monitor data sources for pre-incident indicators and/or behaviors of concern.

Continuously monitor connected systems for sources of threatening or concerning behavior Including localized crime trends, activist group activity, executive name searches, social media activity, and updates to historical cases that trigger a pattern alert	☐
Monitor unusual alerts from connected systems Such as license plate recognition, access controls, or visitor management check-ins	☐
Review alerts from adjacent systems Like intrusion detection, endpoint protection, cyber threat intelligence, and fraud detection	☐
Identify potential risk indicators Indicators could include grievances (internal, external), insider risk awareness feedback programs, connected system alerts, reports (HR, supervisors), casing/surveillance, or law enforcement reports	☐
Identify point of contact (POC) outside of your organization Including local, state, and federal law enforcement, associations, or partner organizations	☐
If a potential threat is identified, trigger escalation and mitigation plans, including notifying and standing up the Insider Threat Working Group	☐

TIP: Information stemming from an insider risk investigation should be made available only to the Insider Risk Working Group. As a critical risk function, it's a key task for this group to decide actions and communicate activity to the appropriate places in an organization.

Incident Intake and Investigation

Capture and prioritize the incident

With the aid of the established protocols, processes, and systems, you can quickly capture the concerns, enabling notification to appropriate stakeholders for further inquiry/investigation, as needed.

Capture the basic details What is the concern, how was it identified, who is the person of interest (POI), when and where did it occur	☐
Set incident priority based on threat level or incident severity	☐
Coordinate appropriate response actions with stakeholders and partners, both internally and externally; record response, if any	☐

Continued on next page

Conduct damage assessment and, as appropriate, engage internal or third-party experts Like IT, engineers, and threat managers	☐
Take immediate containment actions in consideration of physical, informational, or digital risk	☐
Assign lead investigator and/or analyst and initiate investigation workflow	☐

Action investigation steps

Leveraging a consolidated platform for documentation, investigation, and collaboration, you can accelerate detailed investigations to scope, document, and resolve the incident.

Collect relevant information from individuals to understand the concern, the timeline in which it occurred, who was impacted and what parts of the business were disrupted, if any Interview the person who reported the incident and the manager/co-workers of the POI	☐
Collect supporting information to identify a POI, examine their history, establish a timeline of the incident Including prior performance history, criminal history, civil judgments (if authorized and legal), social media, dark web, local and third-party surveillance footage (e.g. building security), email, text or audio information, access controls, surveillance, and travel patterns	☐
Interview the POI Conducted by either HR, legal, security, or police	☐
Analyze previously documented incidents, investigations or crime data to determine if there are any connections or related concerns	☐
Expand notifications as appropriate to internal and external stakeholders Like building security or media relations	☐
Log follow up requirements and communications Including each dispatch, assignment, activity, piece of evidence, or communication between individuals, across functions, or with external third parties	☐
Take any appropriate management actions based on security, HR, and risk management input to contain or mitigate the threat	☐
Take necessary legal and administration actions Work with legal and/or police for trespass warnings and protection orders; limit network activity, lockdown information flows	☐
Re-evaluate incident priority based on threat level or incident severity	☐
Update findings and report to the organization's Insider Risk Working Group Document what has been uncovered, immediate threats, and potential risks; seek guidance, as appropriate	☐
Regularly review and update case disposition status (Open, Closed, Ongoing)	☐

Post-Investigation

Analyze data, metrics and trends

With robust metrics and dashboards, you can analyze risk trends and data to inform preparation and response activities, preserve knowledge, and evolve investigation best practices.

Track investigation data across a wide variety of variables Including case disposition status, case resolution rate, threat type, personnel, and location	☐
Build custom reports against any collected data field or emerging threat signal to gain investigation insights	☐
Define document retention period to ensure you're legally compliant and to guard against re-emergence of issues	☐
Conduct an after action review Consider what happened, what was learned, and what can be done to improve	☐
Set up evaluation dates Trigger a risk review on significant dates (e.g. termination anniversary)	☐