EY Insider Risk Management services

A proactive and data-driven approach

Building a better working world

How safe are your critical assets from insider threats?

An organization's critical assets, both digital and physical, are increasingly exposed through hyper-connectivity of digital and physical assets, perceptions of employee work product entitlement and shifting business structures. This leaves the critical assets of many organizations at increased exposure to an insider threat.

What is insider threat?

An insider threat is a current, temporary or former employee, contractor or business partner who has or had authorized access to an organization's network system, data or premises. The insider may exploit their access to negatively impact the confidentiality, integrity and availability of the organization's critical assets.

The financial, reputational and regulatory impact of having an organization's critical assets compromised, stolen or damaged can be catastrophic. Anyone with trusted access can potentially exploit weaknesses in the monitoring and control environments that protect critical assets, causing millions of dollars of damage. In order to mitigate the risk of insider threats, organizations should establish a formal program to protect their critical assets from compromise.

Technology can play an important role in identifying potential insider threats, but it is not just an IT issue. It takes a collaborative approach — including many human elements — to monitor, detect and mitigate insider threat activities of concern. Managing the risk of insider threat should be considered part of a security program, from both information security and physical security perspectives. However, there are unique challenges that must be addressed, given that insider threats are often hidden in plain sight and are therefore difficult to detect. For example, insider threats:

- Do not need to "break in" because they already have access and knowledge pertaining to the location of critical assets
- Are within an organization's confines, so they are harder to detect via traditional signature-based detection methods

Key components for success

- Gain executive buy-in to formalize scope and scale, secure support from key stakeholders, and create consequence protocols aligned to organizational culture
- Establish repeatable processes to achieve consistency in detecting, investigating and mitigating insider threat activities of most concern to your organization
- Dedicate resources and tools that integrate technical and nontechnical capabilities within an analytics platform to detect insider threats that mature over time
- Prepare for cross-functional collaboration with clearly defined, easy-to-follow procedures, information-sharing protocols and formal training curriculums

Ask better questions

1. Are you taking the right steps to protect your critical assets from insider threats?
2. How do you continually improve your security posture with consideration to insider threats?

Understanding the insider threat landscape

To enable the early detection and rapid mitigation of insider threats, organizations should consider defining the scope and scale of their program by identifying the threat types and potential risk areas that could cause the most harm.

Types of insider threat actors

1	2	3
Malicious	**Compromised**	**Unintentional**
Employees who deliberately cause harm by stealing or damaging critical assets for profit, personal benefit, dissatisfaction or revenge	Employees who have legitimate access to critical assets but who are acting under undue influences	Employees who are well-intentioned but may accidentally disrupt, delete, modify or unwittingly expose critical assets to unauthorized recipients

Examples of areas at most risk to insider threats

Critical asset compromise	▸ Theft ▸ Improper deletion	▸ Manipulation ▸ Unauthorized disclosure
Fraud and criminal activity	▸ Account takeover ▸ Bribery and corruption ▸ Embezzlement	▸ Improper charge-backs ▸ Pay-to-play schemes
Workplace violence	▸ Active shooters ▸ Behavior of concerns	▸ Bullying or harassment ▸ Destruction or sabotage

EY Insider Risk Management approach

EY Insider Risk Management is a dedicated service that helps organizations develop an integrated risk management program to protect their critical assets against insider threats. It offers a data-driven approach that incorporates technical and nontechnical indicators to manage insider threat risks and implements identity analytics, data protection and advanced endpoint monitoring within an analytics platform to identify behaviors of concern for mitigation purposes.

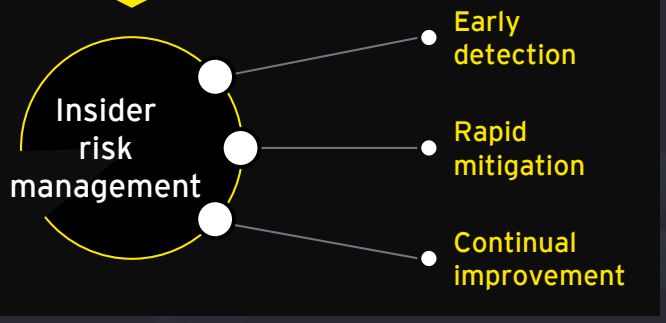
The EY approach was developed by dedicated professionals, who possess a wide range of backgrounds and knowledge in counterintelligence, forensics, data sciences, information security and enterprise risk management with consideration to the following frameworks:

- Executive Order 13587
- US and UK Computer Emergency Response Teams
- Intelligence and National Security Alliance
- National Institute of Standards and Technology
- Centre for the Protection of National Infrastructure
- International Organizations for Standardization 27001 Series

EY professionals created this methodology with the assumption that the insider threat program should be fully integrated with your existing corporate security and cybersecurity programs. Insider threat mitigation should be a part of enterprise-wide risk management considerations and aligned with organizational risk priorities.

Given the nature of the risk, the human element needs to be embedded in every aspect of the insider threat program, from policymaking, monitoring and escalation procedures to consequence protocol management.

EY teams have an insider risk methodology that considers a framework, key regulatory guidance integration with industry frameworks, peer comparisons and leading practices to help organizations develop a successful insider threat program.



EY Insider Risk Management

EY services span the insider risk management life cycle. EY teams work closely with organizations to codevelop integrated insider threat programs that protect critical assets and high-risk positions from a full spectrum of insider threat scenarios.

Successful insider threat programs require the precise balance of due diligence, due care and transparency to build trust and achieve buy-in at appropriate levels throughout your organization. Whether you are just starting out or would like to understand how you compare to peers, EY professionals have services to assist in the development of your insider threat program. EY core services focus on establishing a strong foundation to enhance protections to top-of-mind risk areas and expand as risk priorities evolve — all while providing employees with a clear understanding of the program's objectives to overcome privacy and other cultural concerns.

Service overview

	1 Assess	2 Design	3 Implement	4 Operate	5 Improve
Description	▸ Insider threat program assessment based on EY Insider Threat Maturity Model ▸ Insider threat process assessment (small-scale assessment based on client needs)	▸ Insider threat program/function strategy and road map built to include governance, training, etc. ▸ Insider threat process design (e.g., playbook, governance charter, incident management)	▸ Insider threat program/function implementation ▸ Technology integration where required (e.g., behavioral analytics, data loss prevention) ▸ Insider threat process implementation (e.g., testing process flows)	▸ Operate insider threat investigation protocols to include monitoring, training, committee sessions, etc.	▸ Insider threat program/function optimization based on client maturity and desired end state ▸ Insider threat process optimization
Duration	▸ 2–3 months	▸ 3–6 months	▸ 6–12 months	▸ Continuous	▸ 3–6 months
Benefits	▸ Identification of existing capabilities and gaps ▸ Determination of program maturity level	▸ Established program governance and policies ▸ Defined road map for program enhancements and associated technology	▸ Operational program ▸ Integration of technology solutions ▸ Documented processes for staff	▸ Ongoing support and management of insider threat program activities ▸ Tuning processes based on lessons learned	▸ Technology optimization ▸ Tuning of processes for greater efficiency
Outputs	▸ Maturity assessment report ▸ Target state development	▸ Insider threat policy ▸ Steering committee charter	▸ Procedural documents ▸ Defined service-level objectives	▸ Investigation reports ▸ Training course materials	▸ Data mapping for high-value assets ▸ Documented process flow

The EY advantage

- Battle-tested team leveraging experience in government, national security program protection, counterintelligence, law enforcement, academia, data science, trade secret (IP) protection and behavioral analytics
- Global methodology to build an effective insider threat program around key components of people, process and technology to meet a corporation's needs
- Consistent, phased approach that includes both technical and nontechnical means to mitigate insider threat activities against your critical assets and risk areas
- Global presence in key locations and ability to seamlessly leverage a full spectrum of cyber services to address your insider threat needs

---

Insider risk management team members have strong experience in:

- Federal law enforcement
- Military
- Counterintelligence
- Academia/R&D
- Investigative services
- Physical security
- Background screening
- Forensics
- Security logging and monitoring
- Incident response
- Data governance
- Identity analytics
- Data protection and privacy
- Risk modeling
- Alert management
- Behavior analytics

Technology that supports EY services

Powered by a virtual analytics infrastructure (EY Virtual), a microservices-based AI (artificial intelligence) and forensic data analytics platform, EY Insider Risk Management Services can be deployed on premises or via the cloud, has the scalability to be used in multiple locations, and is capable of integrating with a multitude of data sources, both structured and unstructured.

Deep AI and forensic bench strength

The EY team comprises data science, forensic technology, computer science and cybersecurity professionals who carry not only the academic pedigree but real-world experience in managing data protection and privacy risks. They are experienced at applying AI and forensic technologies and approaches to uncover hidden risk patterns. The EY team also helps clients comply with legal and regulatory requirements and deliver operational effectiveness and efficiencies.

Secure and scalable use environment

EY Virtual provides the accessibility and scalability of a multiuser environment that can accommodate a large number of approved internal and external users. It offers a range of security controls (e.g., role-based permission, two-factor authentication, encryption) to manage data protection and privacy risks. Its multi-tier server architecture is subject to the governance of the EY global information security program, which requires rigid security certification process and multi-layer security monitoring.

Collaborative and interactive case management capabilities

Through EY Virtual's built-in interactive case management tool, compliance professionals have access to a full view of the organization's digital assets. Via a visual dashboard, users can manage alerts, drill into specific risk areas and collaborate with each other in real time. Users can also automate certain escalation procedures using workflow tools. The case manager can integrate a wide range of data sources so that all relevant information needed for an investigation is readily available at one central location.

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

About EY Forensic & Integrity Services

Embedding integrity into an organization's strategic vision and day-to-day operations is critical when managing complex issues of fraud, regulatory compliance, investigations and business disputes. Our international team of more than 4,000 forensic and technology professionals helps leaders balance business objectives and risks, build data-centric ethics and compliance programs, and ultimately develop a culture of integrity. We consider your distinct circumstances and needs to assemble the right multidisciplinary and culturally aligned team for you and your legal advisors. We strive to bring you the benefits of our leading technology, deep subject-matter knowledge and broad global sector experience.

EYG no. 002101-21Gbl
2102-3702241
ED None

ey.com

For more information:

Visit ey.com/Forensics