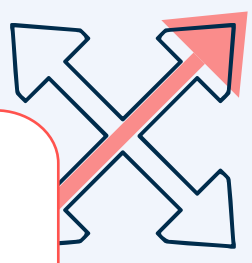
TOP 10 Steps to Achieve a Mature, Whole Person Insider Risk Program

Insider threats refer to harmful actions by trusted individuals who have access to an organization's resources — ranging from sensitive data theft and data exfiltration to sabotage, espionage, fraud, and workplace violence. Thwarting insider threats is challenging, as insiders have legitimate access to sensitive data and have elevated access privileges. To address this growing concern, many organizations are enhancing their program by migrating to a whole person risk assessment approach.

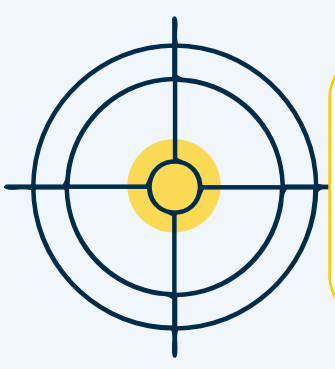
A whole person approach to insider risk management (IRM) incorporates a broad range of user data beyond the monitoring of technical security violations and user activity anomalies. This includes behavioral data ranging from human resources and security information sources to publicly available information such as legal, financial and social records. A recent survey from Cybersecurity Insiders of over 400 cybersecurity professions reveals a growing trend toward this more comprehensive whole person approach.

To help deal with the new information processing and decision making demands, leading programs are applying AI-powered advanced analytics in their insider risk assessment processes.

By analyzing both technical and behavioral data sources, organizations can identify personnel on the critical pathway to insider risk — allowing for preemptive action to prevent or mitigate the risk before an impactful incident occurs. Examine our infographic to discover the top ten steps to achieve a whole person insider risk program.



1. Expand the breadth of stakeholders beyond insider threat security staff to include representatives from human resources, legal, behavioral experts/scientists, and employees. This provides a cross-functional team to better define insider risks, models, requisites, implementation needs, key performance indicators (KPIs) and program enhancements.[3]

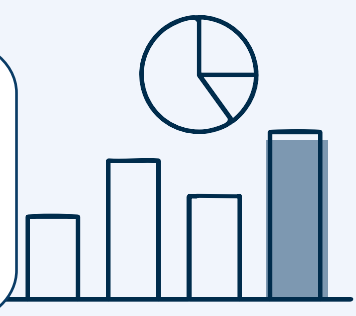


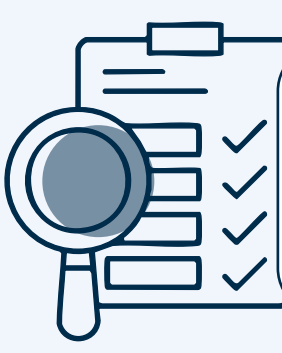
2. Define key insider risks that are of concern to the organization and insider threat assessment processes. Define not only the most egregious threats, but also concerning events, behaviors, and characteristics that help to identify at-risk individuals, preempt impactful incidents, and provide an "offramp" from the critical pathway to insider risk.

3. Identify the technical and behavioral potential risk indicators (PRIs) that could identify people who pose the greatest insider threat risks. This can process can be augmented by leveraging existing PRI taxonomies such as SOFIT — Sociotechnical and Organizational Factors for Insider Threats.[4]

4. Create insider risk assessment models by mapping the sets of PRIs and possible weights (rating scales) of the respective PRIs associated with a specific insider threat behavior. Calibrate the assessment model by applying feedback from internal and expert insider threat analysts.

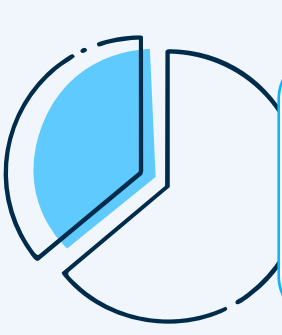
5. Assess and document the sources of technical and behavior data within the organization to identify owners, acquisition methods, frequency and volume, usage limitations, and protection obligations, as well as approval processes. Determine the scope, acceptable risks, and gaps to securely obtain and manage these data sources and maintain compliance.





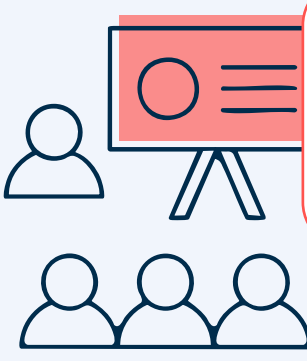
6. Develop monitoring specifications, assessment templates, and response guidance to establish requirements and processes. Identify gaps by comparing current supporting resources, processes, and technologies.

7. Assess current insider risk program metrics and costs across staff and resources, which often are a portion of a security-centered threat detection and response team. Document the number of insider threats identified, investigated and technically resolved, and those requiring more extensive investigation, mitigation and intervention effort. Ideal to estimate any quantitative measures.



8. Ascertain key implementation requirements, costs, operational tradeoffs, and integration must-haves to augment existing tools, controls, and capabilities. Examine the capabilities and costs of new tools and technologies, including the use of expert systems and AI/ML for real-time threat detection and analysis, as well as case management functions that affect analyst workloads from assessment to mitigation.

9. Determine the operational, economic, and risk management improvements by augmenting the current IRM program (underlying resources, processes, and technology) with a whole person approach. Estimate implementation scope, timing, and KPI targets.



10. Document and present key highlights and KPIs to gain stakeholder commitment and move to actionalize plans.

Insiders typically exert multiple actions that lead to an impactful incident. Explained by Frank L Greitzer Ph.D.[5], chief behavioral scientist as Cogility — "traditional approaches focusing only on technical indicators will most often alert security analysts and threat responders only during or after the attack. But if organizations incorporate behavioral factors into their analysis, analysts may observe various tripwires or red flags along the critical pathway".

Cogility Insider Risk Management

Cogility's insider risk management solution provides a whole person approach to detect, prevent, and mitigate insider threats. Cogility continuously monitors and analyzes both technical and behavioral potential risk indicators (PRIs) at machine-speed to identify insider risks with full provenance and explainability. Combined with its advanced case management, Cogility modernizes IRM programs to help organizations more efficiently and effectively respond to and avoid incidents.

For more information, visit **www.cogility.com/insider-risk-management/**.

1 2024 Insider Threat survey by Cybersecurity Insiders n=413

2 Shaw, E. & Sellers, L. (2015). Application of the critical-path method to evaluate insider risks. Studies in Intelligence, 59 (2), 41-48

3 Intelligence and National Security Alliance (INSA), Human Resources and Insider Threat Mitigation: A Powerful Pairing, September 2020 - INSA White Paper

4 SOFIT; Greitzer, Pearl, Leuong, and Becker. **https://ieeexplore.ieee.org/document/8424651**

5 Adapted from: Greitzer et al. (2018). **https://ieeexplore.ieee.org/document/8424651**

COGILITY